

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCHES OF:

SAMSUNG CELLULAR TELEPHONE,
IMEI 350121675480685

Magistrate No. 23-1744

MOTOROLA MOTO G POWER
CELLULAR TELEPHONE, XT2117-1,
SERIAL NUMBER ZY22CTDQM6, IMEI
356889113879890

Magistrate No. 23-1745

CURRENTLY LOCATED AT:

FEDERAL BUREAU OF INVESTIGATION
3311 E. CARSON STREET
PITTSBURGH, PA 15203

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Samantha Shelnick, a Special Agent (SA) with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the examination of property—electronic devices, as described in Attachment A—which are currently in the possession of law enforcement, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have

been so employed since March 2016. I am currently assigned to the Pittsburgh Division of the FBI, Violent Crimes Task Force. In this capacity, I am charged with investigating possible violations of federal criminal law, including the online exploitation of children, which includes violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors, among other violations. By virtue of my position, I have performed a variety of investigative tasks, including the execution of federal search warrants and seizures, and the identification and collection of computer-related evidence. I have participated in the execution of numerous federal search warrants which have involved violations of Title 18, United States Code, Sections 2250, 2251(a), 2252(a), 2422(a) and (b), and 2423—offenses involving the sexual exploitation of children, child sexual abuse material (“CSAM”), and enticement.

3. Based on the information set forth in this affidavit, there is probable cause to believe that on the **TARGET DEVICES** (described more fully below and in Attachment A) there exists fruits, instrumentalities, contraband, and evidence of violation of Title 18, United States Code, Section 2252(a), which makes it a crime to receive, distribute, and possess material depicting the sexual exploitation of a minor (child sexual abuse material/child pornography) and Section 2422(b) which makes it a crime to use a facility or means of interstate commerce, such as the Internet and the telephone, to knowingly attempt to persuade, induce, entice, or coerce an individual who had not attained the age of 18 years to engage in sexual activity for which any person can be charged with a criminal offense.¹ (the “Subject Offenses”).

¹ I am aware that Chapter 31 of Pennsylvania’s Criminal Code, Section 3122.1(b) prohibits a person from engaging in sexual intercourse with an individual under the age of 16 years and that

4. I am requesting authority to search the entirety of the **TARGET DEVICES**, for the items specified in Attachment B, hereto, which items constitute fruits, instrumentalities, contraband, and evidence of the foregoing violations.

5. The facts in this affidavit are based on my personal observations, my training and experience, and information obtained from other agents, witnesses, and sources. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

6. The property to be searched are two cellular devices, described as follows:
- a. Samsung Cellular Telephone, IMEI 350121675480685 (hereinafter **TARGET DEVICE 1**), and
 - b. Motorola Moto G Power Cellular Telephone, XT2117-1, Serial Number ZY22CTDQM6, IMEI 356889113879890 (hereinafter **TARGET DEVICE 2**),
 - c. Hereinafter collectively referred to as the “**TARGET DEVICES.**”

7. The **TARGET DEVICES** are currently located with the Federal Bureau of Investigation at FBI Pittsburgh, 3311 E. Carson Street, Pittsburgh, PA 15203.

8. The applied-for warrants would authorize the forensic examination of the **TARGET DEVICES** for the purpose of identifying electronically stored data particularly described in Attachment B.

person is 11 or more years older than the individual and the person and the individual are not married to each other, and 3123(a)(7) prohibits a person from engaging in deviate sexual intercourse with an individual who is less than 16 years of age and the person is four or more years older than the individual and the individual and the person are not married to each other.

PROBABLE CAUSE

9. On August 4, 2021, in the Commonwealth of Pennsylvania, Allegheny County, a search warrant, incident number CTF#21-027, was issued for the residence located in McKees Rocks, Pennsylvania 15136.² This warrant, attachment, and affidavit are attached hereto as Exhibit 1 and incorporated herein. The search warrant was executed at this residence on August 6, 2021, by members of FBI Pittsburgh's Child Exploitation Task Force, including Allegheny County Police Detective Scott Klobchar, who was the Affiant on the residence search warrant. Pursuant to the search warrant, **TARGET DEVICE 1** was seized and transported to/is maintained in the custody of FBI Pittsburgh's Evidence Control Room located at 3311 E Carson Street, Pittsburgh, Pennsylvania 15203.

10. On September 13, 2021, United States Magistrate Judge Patricia L. Dodge issued Criminal Complaint and Arrest Warrant at Magistrate No. 21-1857, accusing RYAN PETERS of violating Title 18, United States Code, Section 2422(b), which makes it a crime to use a facility or means of interstate commerce, such as the Internet and the telephone, to knowingly attempt to persuade, induce, entice, or coerce an individual who had not attained the age of 18 years to engage in sexual activity for which any person can be charged with a criminal offense. On September 13, 2021, RYAN PETERS was arrested. Pursuant to his arrest, **TARGET DEVICE 2** was seized and transported to/is maintained in the custody of FBI Pittsburgh's Evidence Control Room located at 3311 E. Carson Street, Pittsburgh, Pennsylvania 15203.

² The complete address is known to law enforcement but omitted in accordance with the Court's rules regarding residential addresses.

11. On September 17, 2021, United States Magistrate Judge Patricia L. Dodge issued Search Warrants at Magistrate Nos. 21-1887 and 21-1888 for the **TARGET DEVICES**. These warrants, attachments, and affidavit are attached hereto as Exhibit 2 and incorporated herein.

12. **TARGET DEVICE 1:** Pursuant to the Search Warrant at Magistrate No. 21-1887, and prior to submitting **TARGET DEVICE 1** to FBI personnel for forensic examination, Detective Klobchar manually reviewed **TARGET DEVICE 1**. Detective Klobchar discovered one video depicting a prepubescent female posing naked in sexual acts and/or poses as well as a second video depicting a prepubescent female engaged in vaginal intercourse with an adult male, evidence pertaining to the violation of 18 U.S.C. §§ 2252(a), specifically the possession of CSAM. These videos were located in a Microsoft OneDrive accessible via **TARGET DEVICE 1**.³

13. After manually reviewing **TARGET DEVICE 1**, Detective Klobchar submitted **TARGET DEVICE 1** to FBI personnel to be forensically examined. However, recent attempts to review the forensic examination of **TARGET DEVICE 1** revealed that the examination was not complete as it did not contain the contents which Detective Klobchar witnessed on the device during his manual review of **TARGET DEVICE 1**. Specifically, the forensic examination of **TARGET DEVICE 1** did not contain the Microsoft OneDrive data. By submitting the instant

² On September 30, 2021, in the Commonwealth of Pennsylvania, Allegheny County, a search warrant, incident number CTF#21-027, was issued for the Microsoft OneDrive account discovered on **TARGET DEVICE 1**.³ This warrant, attachment, and affidavit are attached hereto as Exhibit 3 and incorporated herein. A review of the Microsoft OneDrive account revealed several videos depicting CSAM.

It should be noted that at the time of the search warrant for the Microsoft One Drive account, the Allegheny Police Department was investigating PETERS' alleged possession of CSAM. On or about April 25, 2023, the U.S. Attorney's Office for the Western District of Pennsylvania adopted the possession of CSAM charge.

application for a search warrant, I seek authority to search **TARGET DEVICE 1**, by way of requesting FBI personnel to forensically examine **TARGET DEVICE 1** using the now current version of forensic extraction technology in order for me to review the device for evidence of violations of child exploitation, namely violations of 18 U.S.C. §§ 2252(a) and 2422.

14. **TARGET DEVICE 2:** Despite obtaining a Search Warrant at Magistrate No. 21-1888 for **TARGET DEVICE 2**, I recently discovered that **TARGET DEVICE 2** was not forensically examined due to an inadvertent oversight. I submit the instant application for a search warrant to seek authority to search **TARGET DEVICE 2** by way of requesting FBI personnel to forensically examine **TARGET DEVICE 2** using the now current version of forensic extraction technology in order for me to review the device for evidence of violations of child exploitation, namely violations of 18 U.S.C. §§ 2252(a) and 2422.

15. On July 11, 2023, a Grand Jury in the Western District of Pennsylvania returned a Superseding Indictment at Criminal No. 2:21-CR-419, charging PETERS with violating Title 18, United States Code, Section 2422(b) and accusing PETERS of using a facility or means of interstate commerce, such as the Internet and the telephone, to knowingly attempt to persuade, induce, entice, or coerce an individual who had not attained the age of 18 years to engage in sexual activity for which any person can be charged with a criminal offense. The Superseding Indictment at Criminal No. 2:21-CR-419, also charged PETERS with violating Title 18, United States Code, Sections 2252(a)(4)(B), and 2252(b)(2), accusing PETERS of knowingly possessing visual depictions, namely videos in computer graphics and digital files, the production of which involved the use of minors engaging in sexually explicit conduct, and which depicted prepubescent minor and minors who had not attained 12 years of age engaging in sexually explicit conduct, all of which

had been shipped and transported using any means or facility of interstate and foreign commerce, or were produced using materials which had been shipped and transported in interstate and foreign commerce, by any means, including by computer and the Internet.

16. As detailed more thoroughly in the attached Exhibits (and incorporated herein), law enforcement observed CSAM located on **TARGET DEVICE 1** and established that PETERS used **TARGET DEVICE 2** to attempt to entice an individual he believed to be a twelve-year old child. The **TARGET DEVICES** have remained in FBI custody and are in substantially the same condition as when they were originally seized. The FBI takes measures to ensure the integrity of both the electronic devices and the data contained therein in its custody, including the **TARGET DEVICES**.

17. Based upon my training and experience, as well as the training and experience of others I have consulted with, I know that data stored on electronic devices, such as the **TARGET DEVICES**, can persist indefinitely unless a device is damaged or destroyed, or the data is otherwise removed from the device. Even if data is deleted or damaged, a forensic examiner can recover deleted files or traces thereof. Here, there are no indications that the data on the **TARGET DEVICES** or the devices themselves have been damaged or manipulated in any such way as to lessen their evidentiary value. Nor is there any indication that any of the requested records have been deleted since the devices were seized. Thus, there is no reason to believe that the data contained in the **TARGET DEVICES**, or the probable cause supporting the requested search and seizure, is stale.

18. Therefore, I seek renewed authorization for warrants to search the **TARGET DEVICES** for the information described in Attachment B.

19. For the reasons set forth herein, and in the Exhibits, there is probable cause to believe that evidence, fruits, contraband, and instrumentalities of the violations of Title 18, United States Code, Sections 2252 and 2422 are presently located on the **TARGET DEVICES**, described in Attachment A. Thus, there is probable cause to search the property described in Attachment A for evidence, fruits, contraband, and instrumentalities of these crimes further described in attachment B.

20. Nature of examination. Based on the foregoing and based upon the information incorporated from Exhibit 2, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying the **TARGET DEVICES** and would authorize later review of the **TARGET DEVICES** consistent with the warrants. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

21. Manner of execution. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of these warrants does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrants at any time in the day or night.

CONCLUSION

22. Based on the foregoing, I respectfully request that this Court issue search warrants authorizing the examination of the **TARGET DEVICES** described in Attachment A to seek the items described in Attachment B.

23. The above information is true and correct to the best of my knowledge, information and belief.

/s/ Samantha Shelnick
SAMANTHA SHELNICK
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 14th day of November 2023.

THE HONORABLE PATRICIA L. DODGE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The property to be searched are two cellular devices, described as follows:

- (1) Samsung Cellular Telephone, IMEI 350121675480685, and
- (2) Motorola Moto G Power Cellular Telephone, XT2117-1, Serial Number ZY22CTDQM6, IMEI 356889113879890,

currently located with the Federal Bureau of Investigation at FBI Pittsburgh, 3311 E. Carson Street, Pittsburgh, PA 15203. This warrant authorizes the examination of the above-listed property—electronic devices—and the extraction from that property of electronically stored information and items specifically described in Attachment B.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

The particular things to be seized and searched include all records, in whatever format, stored on the Devices, fully described in Attachment A, that relate to violations of 18 U.S.C. §§ 2252(a) (possession of child sexual abuse material/child pornography) and 2422(b) (attempted enticement of a child to engage in sexual activity) (collectively, the “**SPECIFIED FEDERAL OFFENSES**”) and involve **Ryan Peters**, to include:

a. Any records or information, in any format and medium, relating to the **SPECIFIED FEDERAL OFFENSES**.

b. Any and all software and apps, including programs to run operating systems, applications, utilities, compilers, interpreters, and communications programs, including: mapping apps, photography apps, travel apps, email apps, and any applications that have messaging capabilities that are on the Devices.

c. Any and all notes, documents, records, or correspondence, in any format and medium (including e-mail messages, text messages, instant messages, chat logs, and other digital data files) pertaining to location information.

d. In any format and medium, all photographs, images, and videos contained on the Devices.

e. Any and all electronic address books, names, and lists of names and addresses of individuals on the Devices who **Ryan Peters** may have communicated with.

f. Any and all documents, records, or correspondence, pertaining to the ownership and use of the Devices described above, such as saved usernames and passwords, documents,

browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, text messages, photographs, and correspondence.

g. Passwords, encryption keys, and other access devices that may be necessary to access information stored on the Devices or elsewhere. Any and all passwords and other data security devices designed to restrict access to, hide, or destroy software, documentation, or data. Data security devices may consist of software or other programming code. Any and all data which would reveal the presence of malware, viruses or malicious codes located on the computer storage media.

h. Records of, or information about, the Devices’ internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

i. Records evidencing the use of the Internet Protocol Addresses, including records of Internet Protocol Addresses used by the Devices and Internet Protocol Addresses used by computers that the Devices connected to.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Commonwealth of Pennsylvania

APPLICATION FOR
SEARCH WARRANT
AND AUTHORIZATION

COUNTY OF ALLEGHENY

Docket Number
(Issuing Authority):Police Incident
Number: CTF#21-027Warrant Control
Number:

Det. Scott Klobchar

Allegheny County Police Dept

412-432-4095

08/04/2021

AFFIANT NAME

AGENCY

PHONE NUMBER

DATE OF APPLICATION

IDENTIFY ITEMS TO BE SEARCHED FOR AND SEIZED (Be as specific as possible):

*****See Continuation Page 2*****

SPECIFIC DESCRIPTION OF PREMISES AND/OR PERSON TO BE SEARCHED (Street and No., Apt. No., Vehicle, Safe Deposit Box, etc.):

REDACTED St McKees Rocks, PA 15136- According to the Allegheny County Real Estate Portal, this residence is described as a single family residence. The residence is comprised of gray colored siding with a covered front porch.

NAME OF OWNER, OCCUPANT OR POSSESSOR OF SAID PREMISES TO BE SEARCHED (If proper name is unknown, give alias and/or description):

Ryan Mark PETERS, REDACTED

VIOLATION OF (Describe conduct or specify statute):

PACC Sec 6312- Sexual Abuse of Children D

DATE(S) OF VIOLATION:

08/17/2020 through Present

☒ Warrant Application Approved by District Attorney – DA File No. 322419
(If DA approval required per Pa.R.Crim.P. 2002A with assigned File No. per Pa.R.Crim.P. 107)

☒ Additional Pages Attached (Other than Affidavit of Probable Cause)

☒ Probable Cause Affidavit(s) MUST be attached (unless sealed below) Total number of pages: 9

TOTAL NUMBER OF PAGES IS SUM OF ALL APPLICATION, PROBABLE CAUSE AND CONTINUATION PAGES EVEN IF ANY OF THE PAGES ARE SEALED

The below named Affiant, being duly sworn (or affirmed) before the Issuing Authority according to law, deposes and says that there is probable cause to believe that certain property is evidence of or the fruit of a crime or is contraband or is unlawfully possessed or is otherwise subject to seizure, and is located at the particular premises or in the possession of the particular person as described above.

Allegheny County Police Dept

452

Signature of Affiant

Agency or Address if private Affiant

Badge Number

Sworn to and subscribed before me this 4th day of Aug, 2021. Mag. Dist. No. _____

Jul E. Rango Rm 326 Courthouse (SEAL)
Signature of Issuing Authority Office Address

SEARCH WARRANT
TO LAW ENFORCEMENT
OFFICER:

WHEREAS, facts have been sworn to or affirmed before me by written affidavit(s) attached hereto from which I have found probable cause, I do authorize you to search the premises or person described, and to seize, secure, inventory and make return according to the Pennsylvania Rules of Criminal Procedure.

☒ This Warrant shall be served as soon as practicable and shall be served only between the hours of 6AM to 10PM but in no event later than: *

☐ This Warrant shall be served as soon as practicable and may be served any time during the day or night but in no event later than: **
2:18 P M, o'clock Aug 6, 2021

* The issuing authority should specify a date not later than two (2) days after issuance. Pa.R.Crim.P. 2005(d).

** If the issuing authority finds reasonable cause for issuing a nighttime warrant on the basis of additional reasonable cause set forth in the accompanying affidavit(s) and wishes to issue a nighttime warrant, then this block shall be checked. Pa.R.Crim.P. 2006(g).

Issued under my hand this 4th day of Aug 2021 at 2:18 P M, o'clock.

Jul E Rango 5th Jud. Dist 7/1/24 (SEAL)
Signature of Issuing Authority Mag. Dist. or Judicial Dist. No. Date Commission Expires:

Title of Issuing Authority: ☐ District Justice ☒ Common Pleas Judge ☐ _____

☐ For good cause stated in the affidavits(s) the Search Warrant Affidavit(s) are sealed for _____ days by my certification and signature. (Pa.R.Crim.P. 2011)

(Date) (SEAL)

Signature of Issuing Authority (Judge of the Court of Common Pleas or Appellate Court Justice or Judge).

AOPC 410A-11-24-99

TO BE COMPLETED BY THE ISSUING AUTHORITY

EXHIBIT

1

Commonwealth of Pennsylvania

APPLICATION FOR
SEARCH WARRANT
CONTINUATION PAGES

COUNTY OF ALLEGHENY

Docket Number
(Issuing Authority):Police Incident
Number: CTF#21-027Warrant Control
Number:**Continuation of:**☒ Items to be searched
and seized☐ Description of premises/person(s)
to be searched☐ Owner/ Occupant☐ Violations

HARDWARE: All computer hardware and its content, including, but not limited to, any equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical or similar computer impulses or data. Any computer processing units, cellular telephones, internal and peripheral storage devices, (such as fixed disks, external hard disks, floppy disk drives, and diskettes, tape drives, tapes, and optical storage devices), peripheral input / output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers), and related communication devices such as modems, cables, and connections, recording equipment, as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware. These items will be seized and then later searched for evidence relating to the possession, production and / or dissemination of child pornography.

SOFTWARE: Software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word processing, graphics, or spread sheet programs), utilities, compilers, and communications programs. These items will be seized in order to facilitate the search of the computer systems / computer system components / computer systems storage media named above.

DOCUMENTATION: Computer related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items. These items will be seized in order to facilitate the search of the computer systems / computer system components / computer systems storage media named above.

PASSWORDS AND DATA SECURITY DEVICES: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. A password (string of alpha-numeric characters) usually operates as a sort of digital key to unlock particular data security devices. These items will be seized in order to facilitate the search of the computer systems / computer system components / computer systems storage media named above.

Documents: Documents of any nature, electronic, printed, or handwritten which may relate to passwords, accomplices or co-conspirators. Any documents that shows ownership, access and/or control or who resides at the place to be searched more specifically, 247 Marion St McKees Rocks, PA 15136. Child Pornographic images and any other digital evidence relating to the possession and / or dissemination of child pornography, contained on the electronic storage media seized as a result of this search warrant.

Any data, images, electronic communications, and/or any other electronic information contained on, or within, the computer systems/s, computer/s, computer components, cellular telephones, storage media, peripherals, and/or computer software related in any way to any images, photographs, or depictions of Child Pornography (as defined herein and in the section of 6312 of the Pennsylvania Crimes Code). Any and all image and/or video files (conventionally or digitally produced), photographic and video camera equipment (conventional or digital), negatives, slides, video tapes, motion picture films, magazines, books, or drawings of children or adults engaged in sexual activity or sexually suggestive poses or of children nude, semi-nude, or wearing underwear with no outer garment covering the underwear, Any photographs, printed copies, pictures, images, visual representations, or figures depicting Child Pornography (as defined herein and in section 6312 of the Crimes Code).

"Child Pornography" - any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of 18 years engaged in a prohibited sexual act or in the simulation of such act. Prohibited sexual act (as used in section 6312 of the PA Crimes Code) - sexual intercourse, masturbation, sadism, masochism, bestiality, fellatio, cunnilingus, lewd exhibition of the genitals or nudity if such nudity is depicted for the purpose of sexual stimulation or gratification of any person who might view that depiction.

8-4-21

Page 2 of 9 Pages

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number
(Issuing Authority):Police Incident
Number: CTF#21-027Warrant Control
Number:**PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:**

Social security numbers and financial information (e.g. PINS) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.

Your affiant is Detective Klobchar with the Allegheny County Police Department currently assigned to the FBI's Child Exploitation and Human Trafficking Task Force which is comprised of Federal and Local Law Enforcement. Your affiant is also a member of the Delaware County Internet Crimes Against Children (ICAC) Taskforce. Previously your affiant was assigned as a Detective to the Allegheny County Police Department Child Abuse / Sex Assault unit. Your affiant has been in Law Enforcement for over 19 years. I have spent over 11 of those years being assigned to various investigative units within the Allegheny County Police Department to include, narcotics, homicide and child abuse units.

Your affiant is familiar with investigations involving the exploitation of children both via the internet and in person. Your affiant is also familiar with investigations involving child pornography images. As part of my duties, your affiant investigates violations involving online exploitation of children, violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors. Your affiant has participated in the execution of numerous search warrants and arrests relating to sexual abuse of children.

Definition of "Child Pornography" (as defined in section 6312 of the PA Crimes Code) - any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of 18 years engaged in a prohibited sexual act or in the simulation of such act.

Definition of prohibited sexual act (as defined in section 6312 of the PA Crimes Code) - sexual intercourse, masturbation, sadism, masochism, bestiality, fellatio, cunnilingus, lewd exhibition of the genitals or nudity if such nudity is depicted for the purpose of sexual stimulation or gratification of any person who might view that depiction.

IP ADDRESS: An IP address is analogous to a phone number in that both serve as a unique identifier for a particular device. Similar to how a phone number is assigned to a telephone device, an IP address is assigned to a specific computer. Furthermore, each router that a device uses to connect to the Internet also has an IP address assigned by the Internet Service Provider ("ISP"), comparable to how a phone number is assigned by the phone provider. Similar to how a person would dial a given number to reach a specific individual, the assigned IP address allows various devices connected to the Internet to "talk" to each other so that data can be shared among them. Most machines will also have a Domain Name that are easier for people to remember.

Domain Name: This is the unique name that identifies an Internet Site. Domain names always have two or more parts separated by periods. The left side of the domain name is referred to as the *Second Level Domain (SLD)*, while the right side of the Domain Name is referred to as the *Top Level Domain (TLD)*. When you access a website, the domain name is translated to an IP address, which defines the server where the website located. This translation is performed dynamically by a service called DNS, which stands for "Domain Name System."

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

8-4-21



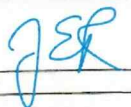
Date

Issuing Authority Signature

Date

(SEAL)

Page 3 of 9 Pages

Commonwealth of Pennsylvania  COUNTY OF ALLEGHENY		AFFIDAVIT OF PROBABLE CAUSE	
Docket Number (Issuing Authority):	Police Incident Number: CTF#21-027	Warrant Control Number:	
PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES: <small>Social security numbers and financial information (e.g. PINS) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.</small>			
<p>Domain names serve as easily memorized names for websites and other services on the Internet. However, computers access Internet devices by their IP addresses. DNS translates domain names into IP addresses, allowing you to access an Internet location by its domain name.</p> <p>American Registry of Internet Numbers (ARIN)- is a non-profit organization, responsible for managing the Internet numbering resources for Canada, the United States, and many Caribbean and North Atlantic islands. Other registry organizations are separately responsible for registering and maintaining domain names, which are commonly used unique identifiers that are translated into numeric addresses (IP Addresses). IP Addresses are globally unique numeric identifiers that computers use to identify hosts and networks connected to the Internet. Open structures and processes are maintained in all of the ARIN's daily operations to ensure that the needs of the Internet Community are adequately met.</p> <p>GOOGLE ACCOUNT: A Google Account is a username and password that can be used to log in to consumer Google applications like Docs, Sites, Maps, and Photos. Many Google accounts end in @gmail.com however it isn't necessary to have a Gmail account in order to have a Google account. Google Photos is a photo sharing and storage service which Google account users can access to share and store photographs and videos.</p> <p>DROPBOX: Dropbox is a file syncing, hosting service that offers cloud storage, file synchronization, personal cloud, and client software access. It allows users to share files on computers, phones, tablets, and the Dropbox website, and permits its users to store files on Dropbox's servers. According to Dropbox's privacy policy, at https://www.dropbox.com/privacy, Dropbox stores, processes and transmits the account holder's files (Including photos, videos, structured data, and emails), which allows users to access any file from anywhere. Dropbox creates a special folder on the user's electronic device, the contents of which are then synchronized to Dropbox's servers and to the other computers and devices that the user has installed Dropbox on, keeping the same files up-to-date on all devices.</p> <p>SNAPCHAT: Snapchat is a multimedia messaging app. One of the key features of Snapchat is that it allows users to share photographs and short video clips between users. One principle feature of Snapchat is that when a photo or video clip is sent, it can only be viewed for a short period of time, before they become inaccessible to the intended recipient. This can be circumvented by photographing the image through external means.</p> <p>National Center For Missing and Exploited Children (NCMEC)- The NCMEC operates the Cyber Tipline which was established by Congress to process reports of child sexual exploitation (including child pornography, online enticement, and contact offenses). The NCMEC reviews these reports and shares them with the appropriate law enforcement agency or Internet Crimes Against Children (ICAC) task force.</p>			
I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.			
 Affiant Signature	8-4-21 Date	 Issuing Authority Signature	(SEAL) Date
Page 4 of 9 Pages			

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number

Police Incident

Warrant Control

(Issuing Authority):

Number: CTF#21-027

Number:

PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:

Social security numbers and financial information (e.g. PINS) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.

In addition to the information provided by the reporting party, NCMEC typically adds geolocation information (if appropriate) and cross-references identifying information such as email address, username, or IP address with existing Cyber Tipline Reports.

On 08/17/2020, the National Center for Missing and Exploited Children (NCMEC) received a Cybertip, (CYBERTIP # 76695176) from Snapchat. Snapchat reported that a user, utilizing the screenname: **jalestal** had uploaded an image of suspected **child pornography** on 08/17/2020 at 05:42:02 UTC. Snapchat provided an **IP Address** that was captured by Snapchat on 08/14/2020 at 02:50:24 UTC, and identified that **IP Address: 72.65.243.155**. Snapchat also reported that this account was associated with cellular telephone number (412) 512-6248.

Your affiant viewed the uploaded image and confirmed that it depicted a *prepubescent female child* exposing her genitals in a sexual act and/or pose.

On 09/16/2020, the National Center for Missing and Exploited Children (NCMEC) received a Cybertip, (CYBERTIP # 79623247) from Dropbox. Dropbox reported to NCMEC that a person using the Screen/User Name: **Jalestal Divine**, uploaded *eleven (11) images* of suspected **child pornography** to their Dropbox account. Dropbox provided that this user registered this Dropbox account using **IP address: REDACTED 155** on 08-03-2020 at 22:08:18 UTC. Dropbox identified the Email account associated with this account as: **jalestal1@gmail.com**.

Dropbox reported that they had viewed the entire contents of the uploaded files. Your affiant also previewed the reported uploaded files and confirmed that they depicted *prepubescent aged female children* engaged in sexual acts and/or exposing their genitals in a sexual act and/or pose.

Based on the fact that the National Center for Missing and Exploited Children (NCMEC), had reported receiving two separate **Cybertips** from different electronic service providers, which reported the same **IP Address of: REDACTED 155**, it was believed by your affiant that both accounts were operated by a single user. A check of the **IP Address: REDACTED 155** through *IP2Location.com*, yielded results for belonging to **Verizon communications**.

On 04/29/2021, a search warrant was applied for and obtained for the subscriber information on the **IP Address: REDACTED 155**. The search warrant was signed by the Honorable Judge David Cashman. The search warrant was executed on **Verizon communications** and as a result, **Verizon** provided the following information.

Verizon provided the subscriber information as, **REDACTED REDACTED**, with a service address of **REDACTED REDACTED** in **St McKees Rocks, PA 15136** and provided an email that was linked to the **Verizon** account, which **Verizon** identified as, **jalestal1@gmail.com**. According to **Verizon** records, the address of **REDACTED REDACTED** **St McKees Rocks, PA 15136**, would have been the service address of **IP Address: REDACTED 155** at the time both **Cybertips** were reported.

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

Affiant Signature

8-4-21
Date

Issuing Authority Signature

Date

(SEAL)

Page 5 of 9 Pages

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number
(Issuing Authority):Police Incident
Number: CTF#21-027Warrant Control
Number:

PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:

Social security numbers and financial information (e.g. PINS) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.

Investigators began gathering intelligence on current potential residents, residing at [REDACTED] [REDACTED] St McKees Rocks, PA 15136. As a result, it was learned that, **Ryan Mark PETERS**, was listed as currently residing at this address. A check of **PETERS** through JNET, yielded [REDACTED] [REDACTED] St McKees Rocks, PA 15136 as the address, he lists on his Pennsylvania Driver's License. On 07/26/2021 US Postal Inspectors confirmed that **Ryan PETERS** and [REDACTED] [REDACTED] are currently receiving US Mail at this address.

A criminal history check of **PETERS**, reflected that he has prior arrests in New York and Pennsylvania, to include a **2013 Pennsylvania arrest for the following offenses: Statutory Sexual Assault, Aggravated Indecent Assault, Unlawful contact with a minor, Corruption of Minors, and IDSI**. A criminal complaint was obtained regarding the aforementioned charges. Upon reviewing the criminal complaint, it was learned that on 03/07/2013, the **Pennsylvania State Police** filed the above charges, subsequent to an investigation, in which **PETERS** was alleged to have engaged in sexual intercourse with a 13 year-old female, when he was 22 years-old.

A check of the telephone number, [REDACTED] 6248, through a law enforcement database, yielded results for belonging to **Ryan M PETERS**, [REDACTED] (1989) of [REDACTED] [REDACTED] St McKees Rocks, PA 15136.

Based on the fact that both Cybertips were associated with screen name, "**Jalestal**", I conducted a check of the screenname **JALESTAL** through **Facebook**, to determine if that username was associated with a **Facebook** account. As a result, I located a **Facebook** page under the name, "**Ryan Jalestal Peters**". This **Facebook** account displayed a **Facebook** profile picture that was extremely similar to the driver's license photograph of **Ryan M. PETERS**, [REDACTED] (1989). In the "about" section of the **Facebook** profile, it stated that he attended **Clymer Central School**. While reviewing the previously mentioned criminal complaint, filed on 03/07/2013, the complaint states that **PETERS** had stated that he graduated from high school in **Clymer, NY**.

Based upon your affiant's training and years of experience as a police officer, your affiant knows that images/videos of child pornography are often stored in computers. The images and or video themselves may be stored as electronic data and as files on various types of media, including but not limited to hard drives, zip drives, floppies, tape drives and tapes.

Based on your affiant's knowledge, training, and experience, your affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data.

Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

Affiant Signature _____ Date 8-4-21 Issuing Authority Signature JER Date _____ (SEAL)
Page 6 of 9 Pages

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number

Police Incident
Number: CTF#21-027Warrant Control
Number:

(Issuing Authority):

PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:

Social security numbers and financial information (e.g. PINs) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.

to a set block of storage space for long periods of time before they are overwritten.

In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve remnants of an electronic file from a hard drive depends less on when the file was downloaded or viewed and more on the user's operating system, storage capacity, and computer habits.

Based on your affiant's knowledge, training, and experience, your affiant knows that child pornographers generally, prefer to store images of child pornography in electronic form as computer files. The computer's ability to store images in digital form makes a computer an ideal repository for pornography. A small portable disk can contain hundreds or thousands of images of child pornography, and a computer hard drive can contain tens of thousands of such images at very high resolution. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child pornography and the disks that contain the files can be mislabeled or hidden to evade detection.

Based upon your affiant's knowledge, training and experience, your affiant knows that searching and seizing information from computers often requires officers to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

- 1) The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks) can store the equivalent of millions of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.
- 2) Technical Requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password protected, or encrypted files.

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

(SEAL)

Affiant Signature

Date

Issuing Authority Signature

Date

Page 7 of 9 Pages

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number
(Issuing Authority):Police Incident
Number: CTF#21-027Warrant Control
Number:**PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:**

Social security numbers and financial information (e.g. PINS) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.

Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis. Further, such searches often require the seizure of most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

In light of these concerns, your affiant hereby requests the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the officers executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence. Accordingly, if any computers/cellular smartphones are found, said computers/cellular smartphones are to be seized and subsequently searched.

The evidence sought by this search warrant is believed to be present due to the fact that people with collections of child pornography keep their collection for long periods of time, years at times. Even if the child pornography was deleted, a Computer Crime unit or any other trained Forensic examiner can recover deleted files long after the files have been deleted. The staleness of digital evidence had been addressed in the federal court system numerous times:

U.S. v. Lacy (9th Cir. 1997) 119 F.3d 742. Given nature of the crime, good reason to believe the computerized visual depictions downloaded would be found in def.'s apt. 10 months later. Def. identified as a "collector of child porn."

U.S. v. Sassani (4th Cir. 1998) 139 F.3d 895 (unpublished disposition). Def. failed to support his contention that the search warrant affidavit containing Lanning's profile of a child pornographer was required to meet the standards of Daubert (1993) 509 U.S. 579. Search warrant info found not stale where def. transmitted porn on several separate occasions between 1994 and 1995, most recently four separate transmissions on 3/11/95; search warrant obtained 9/19/95. Also, search warrant found to be sufficiently particular (allowed seizure of "any [specific types of equipment listed] equipment which could be used to depict, distribute, possess, or receive child porn").

U.S. v. Winningham (D. Minn. 1996) 953 F. Supp. 1068. 1985—convicted of sexual improprieties w/children; 6 weeks before search warrant, had collection of photos of young girls w/whip-like marks & letters written to young girls, in one def. admitted infantilism was his thing. SW sought 12/26/95; not stale.

Your affiant believes that images of Child Pornography will be found on the computer's, cellular phone and/or other storage media located at **REDACTED** McKees Rocks, PA 15136., which will lead to the identity of the individual/s who possess child pornography.

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

[Signature] *8-4-21* *[Signature]* *[Signature]* (SEAL)
Affiant Signature Date Issuing Authority Signature Date
Page 8 of 9 Pages

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number
(Issuing Authority):Police Incident
Number: CTF#21-027Warrant Control
Number:

PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:

Social security numbers and financial information (e.g. PINS) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.

Your affiant believes that there is probable cause to believe that these items constitute evidence and instrumentalities of violation for the crime of **Title 18, Section 6312, Sexual Abuse of Children**. Your affiant learned through training and experience, those persons engaged in the distribution and possession of pornographic/child pornographic materials often maintain collections of such material for long periods of time even years at times, as they are considered to be highly valuable to the offender. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials in the furtherance of child exploitation to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts, they want the child victim to perform.

I am respectfully requesting a search warrant for the residence of [REDACTED] [REDACTED] **St McKees Rocks, PA 15136** for the items outlined in this affidavit. Your affiant asserts the named items are evidence of criminal activity and as such are subject to search and seizure.

7ER

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.


Affiant Signature

8-4-21
Date


Issuing Authority Signature

8/4/21
Date

(SEAL)

Page 9 of 9 Pages

UNITED STATES DISTRICT COURT

for the

Western District of Pennsylvania

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))SAMSUNG CELLULAR TELEPHONE, IMEI
350121675480685)

Case No. Magistrate 21-1887

[UNDER SEAL]

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Western District of Pennsylvania
(identify the person or describe the property to be searched and give its location):

Please see Attachment A, Target Item 1, incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Please see Attachment B, incorporated herein.

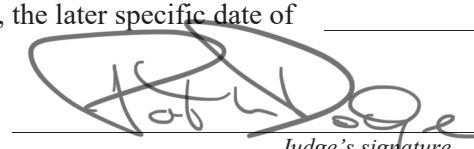
YOU ARE COMMANDED to execute this warrant on or before October 1, 2021 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Duty Magistrate Judge.

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of .Date and time issued: 09/17/2021 12:30 pm


Judge's signature

City and state: Pittsburgh, Pennsylvania

Hon. Patricia L. Dodge, U.S. MAGISTRATE JUDGE

Printed name and title

EXHIBIT

2

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return		
Case No.: Magistrate 21-1887	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED (TARGET ITEMS)

- (1) Samsung Cellular Telephone, IMEI 350121675480685,
- (2) Motorola Moto G Power Cellular Telephone, XT2117-1, Serial Number ZY22CTDQM6, IMEI 356889113879890,
- (3) LG K51 Cellular Telephone, LM-K500UM, Serial Number 009WIRW2724902, IMEI 354591111029583,
- (4) Samsung Galaxy A11 Cellular Telephone, SM-A115U, Serial Number R95N80MQ1ZM, IMEI 356425115244151, and
- (5) 2015 Chevrolet Sonic Sedan, License Plate LPR2231, Vehicle Identification Number (VIN) 1G1JC5SH9F4180911 (“the **TARGET ITEMS**”).

This warrant authorizes the examination of the above-listed property—electronic devices and a vehicle—and the extraction from that property of electronically stored information and items specifically described in Attachment B.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

The particular things to be seized and searched include all records, in whatever format, stored on the **TARGET DEVICES** or in the **TARGET VEHICLE**, fully described in Attachment A that relate to 18 U.S.C. § 2252(a), relating to the possession of child pornography, and 18 U.S.C. § 2422(b), enticement, and involve PETERS, to include:

1. Any depictions of child pornography as defined in 18 U.S.C. § 2256(8), any visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), and any child erotica.

2. Any and all software and apps, including programs to run operating systems, applications, utilities, compilers, interpreters, and communications programs, including: mapping apps, photography apps, travel apps, email apps, and any applications that have messaging capabilities.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including e-mail messages, text messages, instant messages, chat logs, and other digital data files) pertaining to location information.

4. In any format and medium, all photographs, images, and videos contained on the **TARGET DEVICES**.

5. Any and all electronic address books, names, and lists of names and addresses of individuals on the **TARGET DEVICES** who PETERS may have communicated with.

6. Any and all documents, records, or correspondence, pertaining to the ownership and use of the **TARGET DEVICES** described above, such as saved

usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, text messages, photographs, and correspondence, including the text messages with the undercover described in this affidavit or with anyone else in violation of 18 U.S.C. § 2422(b).

7. Passwords, encryption keys, and other access devices that may be necessary to access information stored on the **TARGET DEVICES** or elsewhere. Any and all passwords and other data security devices designed to restrict access to, hide, or destroy software, documentation, or data. Data security devices may consist of software or other programming code. Any and all data which would reveal the presence of malware, viruses or malicious codes located on the computer storage media.

8. Records of, or information about, the **TARGET DEVICES’** internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

9. Records evidencing the use of the Internet Protocol Addresses, including records of Internet Protocol Addresses used by the device and Internet Protocol Addresses used by computers that the **TARGET DEVICES** connected to.

10. Items evidencing a violation of 18 U.S.C. § 2422(b) located in the **TARGET VEHICLE** which were specifically discussed during conversations between PETERS and the undercover, to include, but not limited to, condoms.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search for the **TARGET DEVICES**, described in Attachment A, law enforcement personnel are authorized if necessary, to (1) press or swipe Ryan Peters' fingers (including thumbs) to the fingerprint scanner of the **TARGET DEVICES**; and (2) present Ryan Peters' face to the camera of the **TARGET DEVICES** found in the possession of Peters for the purpose of attempting to activate the facial recognition feature and unlock the **TARGET DEVICES** via biometric security in order to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the

Western District of Pennsylvania

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))

Case No. Magistrate 21-1888

MOTOROLA MOTO G POWER CELLULAR TELEPHONE,
XT2117-1, SERIAL NUMBER ZY22CTDQM6, IMEI
356889113879890)

[UNDER SEAL]

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Western District of Pennsylvania
(identify the person or describe the property to be searched and give its location):

Please see Attachment A, Target Item 2, incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Please see Attachment B, incorporated herein.

YOU ARE COMMANDED to execute this warrant on or before October 1, 2021 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Duty Magistrate Judge
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of .Date and time issued: 09/17/2021 12:30 pm


Judge's signature

City and state: Pittsburgh, Pennsylvania

Hon. Patricia L. Dodge, U.S. MAGISTRATE JUDGE

Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return		
Case No.: Magistrate 21-1888	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 60%;"> <p style="text-align: center;">_____ <i>Executing officer's signature</i></p> <p style="text-align: center;">_____ <i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED (TARGET ITEMS)

- (1) Samsung Cellular Telephone, IMEI 350121675480685,
- (2) Motorola Moto G Power Cellular Telephone, XT2117-1, Serial Number ZY22CTDQM6, IMEI 356889113879890,
- (3) LG K51 Cellular Telephone, LM-K500UM, Serial Number 009WIRW2724902, IMEI 354591111029583,
- (4) Samsung Galaxy A11 Cellular Telephone, SM-A115U, Serial Number R95N80MQ1ZM, IMEI 356425115244151, and
- (5) 2015 Chevrolet Sonic Sedan, License Plate LPR2231, Vehicle Identification Number (VIN) 1G1JC5SH9F4180911 (“the **TARGET ITEMS**”).

This warrant authorizes the examination of the above-listed property—electronic devices and a vehicle—and the extraction from that property of electronically stored information and items specifically described in Attachment B.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

The particular things to be seized and searched include all records, in whatever format, stored on the **TARGET DEVICES** or in the **TARGET VEHICLE**, fully described in Attachment A that relate to 18 U.S.C. § 2252(a), relating to the possession of child pornography, and 18 U.S.C. § 2422(b), enticement, and involve PETERS, to include:

1. Any depictions of child pornography as defined in 18 U.S.C. § 2256(8), any visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), and any child erotica.

2. Any and all software and apps, including programs to run operating systems, applications, utilities, compilers, interpreters, and communications programs, including: mapping apps, photography apps, travel apps, email apps, and any applications that have messaging capabilities.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including e-mail messages, text messages, instant messages, chat logs, and other digital data files) pertaining to location information.

4. In any format and medium, all photographs, images, and videos contained on the **TARGET DEVICES**.

5. Any and all electronic address books, names, and lists of names and addresses of individuals on the **TARGET DEVICES** who PETERS may have communicated with.

6. Any and all documents, records, or correspondence, pertaining to the ownership and use of the **TARGET DEVICES** described above, such as saved

usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, text messages, photographs, and correspondence, including the text messages with the undercover described in this affidavit or with anyone else in violation of 18 U.S.C. § 2422(b).

7. Passwords, encryption keys, and other access devices that may be necessary to access information stored on the **TARGET DEVICES** or elsewhere. Any and all passwords and other data security devices designed to restrict access to, hide, or destroy software, documentation, or data. Data security devices may consist of software or other programming code. Any and all data which would reveal the presence of malware, viruses or malicious codes located on the computer storage media.

8. Records of, or information about, the **TARGET DEVICES’** internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

9. Records evidencing the use of the Internet Protocol Addresses, including records of Internet Protocol Addresses used by the device and Internet Protocol Addresses used by computers that the **TARGET DEVICES** connected to.

10. Items evidencing a violation of 18 U.S.C. § 2422(b) located in the **TARGET VEHICLE** which were specifically discussed during conversations between PETERS and the undercover, to include, but not limited to, condoms.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search for the **TARGET DEVICES**, described in Attachment A, law enforcement personnel are authorized if necessary, to (1) press or swipe Ryan Peters' fingers (including thumbs) to the fingerprint scanner of the **TARGET DEVICES**; and (2) present Ryan Peters' face to the camera of the **TARGET DEVICES** found in the possession of Peters for the purpose of attempting to activate the facial recognition feature and unlock the **TARGET DEVICES** via biometric security in order to search the contents as authorized by this warrant.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCHES OF:

SAMSUNG CELLULAR TELEPHONE, IMEI
350121675480685

MOTOROLA MOTO G POWER CELLULAR
TELEPHONE, XT2117-1, SERIAL NUMBER
ZY22CTDQM6, IMEI 356889113879890

LG K51 CELLULAR TELEPHONE, LM-
K500UM, SERIAL NUMBER
009WIRW2724902, IMEI 354591111029583

SAMSUNG GALAXY A11 CELLULAR
TELEPHONE, SM-A115U, SERIAL NUMBER
R95N80MQ1ZM, IMEI 356425115244151

2015 CHEVROLET SONIC SEDAN, LICENSE
PLATE LPR2231, VEHICLE
IDENTIFICATION NUMBER (VIN)
1G1JC5SH9F4180911

Magistrate No. 21-1887
[UNDER SEAL]

Magistrate No. 21-1888
[UNDER SEAL]

Magistrate No. 21-1889
[UNDER SEAL]

Magistrate No. 21-1890
[UNDER SEAL]

Magistrate No. 21-1891
[UNDER SEAL]

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Samantha Shelnick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices and a vehicle—and the extraction from that property of electronically stored information and items specifically described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so employed since March 2016. I am currently assigned to the Pittsburgh Division of the FBI, Violent Crimes Task Force. In this capacity, I am charged with investigating possible

violations of federal criminal law, including the online exploitation of children, which includes violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors, among other violations. I have participated in the execution of numerous federal and state search warrants which have involved child sexual exploitation and/or child pornography offenses. By virtue of my position, I perform and have performed a variety of investigative tasks, including the execution of federal search warrants and seizures, and the identification and collection of computer-related evidence. I have personally participated in the execution of numerous federal arrest warrants, search warrants involving the search and seizure of computer equipment in cases involving violations of Title 18, United States Code, Sections 2250, 2251(a), 2252(a), 2422(a) and (b), and 2423—offenses involving the sexual exploitation of children, child pornography, and enticement.

3. This affidavit is made in support of an application for a search warrant to search digital devices, more specifically cellular telephones, and a vehicle, for criminal offenses in violation of Title 18, United States Code, Section 2252(a), which makes it a crime to receive, distribute, and possess material depicting the sexual exploitation of a minor (child pornography) and Section 2422(b) which makes it a crime to use a facility or means of interstate commerce, such as the Internet and the telephone, to knowingly attempt to persuade, induce, entice, or coerce an individual who had not attained the age of 18 years to engage in sexual activity for which any person can be charged with a criminal offense.¹ (the “Subject Offenses”). The

¹ I am aware that Chapter 31 of Pennsylvania’s Criminal Code, Section 3122.1(b) prohibits a person from engaging in sexual intercourse with an individual under the age of 16 years and that person is 11 or more years older than the individual and the person and the individual are not married to each other, and 3123(a)(7) prohibits a person from engaging in deviate sexual intercourse with an individual who is less than 16 years of age and the person is four or more years older than the individual and the individual and the person are not married to each other.

property to be searched are a (1) Samsung Cellular Telephone, IMEI 350121675480685, (2) Motorola Moto G Power Cellular Telephone, XT2117-1, Serial Number ZY22CTDQM6, IMEI 356889113879890, (3) LG K51 Cellular Telephone, LM-K500UM, Serial Number 009WIRW2724902, IMEI 354591111029583, (4) Samsung Galaxy A11 Cellular Telephone, SM-A115U, Serial Number R95N80MQ1ZM, IMEI 356425115244151 (the **TARGET DEVICES**), and (5) 2015 Chevrolet Sonic Sedan, License Plate LPR2231, Vehicle Identification Number (VIN) 1G1JC5SH9F4180911 (“**TARGET VEHICLE**”) (“the **TARGET DEVICES** and **TARGET VEHICLE** will collectively hereinafter be referred to as the “**TARGET ITEMS**”), as described in Attachment A, which is attached hereto and incorporated by reference, for evidence of the Subject Offenses, as set forth in Attachment B, which is attached hereto and incorporated herein.

4. The facts in this affidavit are based on my personal observations, my training and experience, and information obtained from other agents, witnesses, and sources. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

FACTS ESTABLISHING PROBABLE CAUSE

5. On August 26, 2021, an undercover agent created an account on an Internet-based application which is a geosocial networking and online dating application. It runs on iOS and Android devices and is available for download from the Apple App Store and Google Play. Users can tap on the picture of another social media user, and the app will display a brief profile for that user, as well as the option to chat, send pictures, and share one's precise location.

6. In this investigation, the undercover assumed the identity of a twelve-year-old female located in Pittsburgh, Pennsylvania. An individual with the social media username

“Jalestal Aka Acerak” from McKees Rocks, Pennsylvania contacted the undercover via the app and engaged the undercover in a private messaging conversation on August 26, 2021 at or around 8:00 PM. Between the dates of August 26, 2021 and August 28, 2021, social media user “Jalestal Aka Acerak” contacted the undercover several times via private messaging on the social media platform and via phone text messages.

7. Social media user “Jalestal Aka Acerak” had a profile picture as well as several other pictures of himself available to view in the application. Upon review of the social media user “Jalestal Aka Acerak’s” pictures, the undercover recognized the individual as RYAN PETERS (herein referred to as “PETERS”). And the undercover recognized social media user “Jalestal Aka Acerak” as a subject of a previous investigation involving Violent Crimes Against Children.

8. As a part of the previous investigation, social media and file sharing platforms reported to the National Center for Missing and Exploited Children (NCMEC) that an individual using the screennames “Jalestal” and “Jalestal Divine” uploaded images of purported Child Sexual Assault Material (CSAM) to their platforms. Additionally, the user with screenname “Jalestal” registered their account on the social media platform with the email address samuelfitgerald408@gmail.com.

9. At least some of the purported CSAM images were uploaded via an IP address resolving to a residence in McKees Rocks, Pennsylvania. Upon execution of a search warrant²

² The search warrant, incident number CTF#21-027, was issued on August 4, 2021 in the Commonwealth of Pennsylvania, Allegheny County for the residence located at [REDACTED] [REDACTED] Street, McKees Rocks, Pennsylvania 15136. The search warrant was executed at this residence on August 6, 2021 by FBI Pittsburgh’s Child Exploitation Task Force. **TARGET DEVICE 1** was seized, entered in to, and maintains in the custody of the FBI Pittsburgh Evidence Control Room located at 3311 E Carson Street, Pittsburgh, PA 15203.

at this residence, law enforcement officers encountered PETERS as a resident of the home.

PETERS provided biographical and contact information including his email account

samuelfitgerald408@gmail.com.

10. Pursuant to the search warrant executed at PETERS' residence, Samsung Cellular Telephone, IMEI 350121675480685 (**TARGET DEVICE 1**) was seized. **TARGET DEVICE 1** was unable to be forensically accessed as the device requires biometric authorization and the pin code is unknown to investigators.

11. Here, with respect to the present investigation, PETERS requested the undercover's telephone number and sent the undercover a text message to continue conversing via text message. The telephone number via which PETERS text messaged the undercover was (814) 427-0507. Database searches of the telephone number (814) 427-0507 revealed that this phone number is registered to RYAN PETERS.

12. On August 26, 2021 at approximately 8:11 PM, PETERS contacted the undercover on social media and asked "Hey, what's up," to which the undercover replies "Hey u." PETERS continued to engage the undercover on August 26, 2021 at approximately 8:11 PM. The undercover responded at 10:16 PM. PETERS continued to engage the undercover:

08/26/2021– PETERS – So your 4'11 I love that height

08/26/2021– UC – Haha ya im still small. wbu

08/26/2021– PETERS – I'm 5'7 and hey you're that super fun size

08/26/2021– PETERS – 😊

08/26/2021– UC – Haha I dunno bout tht

08/26/2021– PETERS – Well I can pick u up which is super cute. Plus if u need someone to shop with I can help. And I love kissing a woman shorter then me

08/26/2021– PETERS – Question is are you single

08/26/2021– PETERS – Oh and I do drive

The conversation continues and PETERS asks the undercover:

08/26/2021– PETERS – Cool 😊 so would u wanna be my girlfriend

08/26/2021– UC – I dunno yet haha how old r u

08/26/2021– PETERS – 24 u?

08/26/2021– UC – Ohhh

08/26/2021– PETERS – How old are you

08/26/2021– UC – I'll be 13 next month but don't report me please. I don't wanna get banned

08/26/2021– PETERS – Ah, ok I won't. So what are u looking for on here

08/26/2021– UC – Ok 😊 😊 I don't know I just joined n saw ur message

08/26/2021– UC – I liked ur tattoo

08/26/2021– UC – I want one when I'm oldr

08/26/2021– PETERS – Yeah just tell people you are 18. And thanks. So what all have you done before with a boy and awesome

13. The conversation continues and PETERS asks the undercover:

08/26/2021– PETERS – Do u wanna have sex

08/26/2021– UC – I don't wanna get hurt or pregnant

08/26/2021– PETERS – If I could promise neither would happen

08/26/2021– UC – Wdu mean

08/26/2021– PETERS – That you wouldn't get hurt or pregnant

08/26/2021– UC – How can u promise that

08/26/2021– PETERS – Cause I have taken a few virginities before and I can't get anyone pregnant

08/26/2021– UC – U have n they didn't get pregnant? What about pain? I heard it hurts. I'm sorry 4 askin I just get scared

08/26/2021– PETERS – It does if they guy doesn't know what he's doing

14. PETERS later says to the undercover that maybe they can meet sometime. The undercover responds:

08/26/2021– UC – Ya that be cool if u think

08/26/2021– UC – What can we do

08/26/2021– PETERS – I'd love to kiss you all over

08/26/2021– UC – Really?!

08/26/2021– PETERS – Yeah if you’d let me

08/26/2021– UC – As long as I dont get busted. I just got my phone back haha

08/26/2021– PETERS – I’ll give you a massage while u are naked and kiss you all over
And no I wouldn’t want u to get busted

15. On August 27, 2021 at approximately 2:26 PM the conversation continues:

08/27/2021– UC – My mom is always checking for apps n stuff so mb we can text. Thays
easier to hide bc I can delete them

08/27/2021– PETERS – Ok what’s your number

08/27/2021– UC – Omg R u sure haha

08/27/2021– PETERS – Yeah

16. PETERS requested the undercover’s telephone number and on August 27, 2021 at
approximately 2:50 PM, PETERS sent the undercover a text message from telephone number
(814) 427-0507. PETERS then continues to engage in conversation with the undercover:

08/27/2021 3:46 PM – PETERS – Ok, so u wanna c me soon

08/27/2021 3:47 PM – UC – I was gonna ask u the same thing haha. Soooo

08/27/2021 3:47 PM – PETERS – I do

08/27/2021 3:47 PM – UC – Can I ask u a ?

08/27/2021 3:47 PM – PETERS – Sure

08/27/2021 3:47 PM – UC – K

08/27/2021 3:48 PM – UC – Did u mean everything u said last nite

08/27/2021 3:48 PM – PETERS – Yeah I did

PETERS then asks the undercover:

08/27/2021 3:49 PM – PETERS – You want me to be your first?

08/27/2021 3:50 PM – UC – R u sure its ok

08/27/2021 3:51 PM – PETERS – Yeah, do u want me to be your first

08/27/2021 3:52 PM – UC – Im just really nervous

08/27/2021 3:53 PM – PETERS – I promise I won't hurt you or get you pregnant

08/27/2021 3:53 PM – UC – K 😊

08/27/2021 3:54 PM – PETERS – So you want me to be your first?

08/27/2021 3:54 PM – UC – Yeah if u r sure I wont get hurt k

08/27/2021 3:55 PM – PETERS – Yes I am sure

08/27/2021 3:55 PM – UC – I trust you

08/27/2021 3:55 PM – PETERS – I love you

08/27/2021 3:56 PM – PETERS – I will be gentle

17. PETERS continues to engage the undercover in conversation:

08/27/2021 4:54 PM – PETERS – Your dad gonna be there all weekend

08/27/2021 4:55 PM – UC – I dunno yet. I'll find out

08/27/2021 4:56 PM – UC – Y

08/27/2021 4:59 PM – PETERS – 😊

08/27/2021 5:00 PM – PETERS – Ok if he isn't there wanna see me

08/27/2021 5:01 PM – UC – Where we gonna go

08/27/2021 5:00 PM – PETERS – My place if u want

08/27/2021 5:00 PM – PETERS – Ok if he isn't there wanna see me

18. On August 27, 2021 at approximately 7:44 PM, PETERS tells the undercover:

08/27/2021 7:44 PM – PETERS – Well stay at your dad's on Sunday and have your mom come get u Monday

08/27/2021 7:44 PM – UC – My dad likes me at his place when he is gone cuz my mum is a nurse n works 12 hr shifts

08/27/2021 7:45 PM – PETERS – Then that will be perfect, I can get u when he leaves

08/27/2021 7:45 PM – PETERS – Would it be later in the day you think

08/27/2021 7:45 PM – UC – Wht if it ain't til late

08/27/2021 7:46 PM – PETERS – That's fine babe

08/27/2021 7:47 PM – PETERS – U gonna wear any panties pr a bra?

08/27/2021 7:47 PM – UC – I hv school Monday n I get the 6th n 7th grade bus which is earlier than HS 4 some reason

08/27/2021 7:48 PM – UC – When?

08/27/2021 7:48 PM – PETERS – When u see me, and that's fine babe I'll get u back before too late

08/27/2021 7:48 PM – UC – U sure?

08/27/2021 7:49 PM – PETERS – Yes I promise, please don't wear a bra or panties please babe

08/27/2021 7:48 PM – PETERS – When u see me, and that's fine babe I'll get u back before too late

19. PETERS then says to the undercover:

08/27/2021 8:47 PM – PETERS – Oh once u and I make love the first time you'll be able to have me inside u anytime and place u want babe

08/27/2021 8:49 PM – UC – R u serious Sam?

08/27/2021 8:49 PM – PETERS – Yeah

08/27/2021 8:49 PM – PETERS – Would u like that REDACTED

08/27/2021 8:51 PM – PETERS – 😊

08/27/2021 8:53 PM – PETERS – That would be amazing my love

08/27/2021 8:53 PM – PETERS – My forever

08/27/2021 8:53 PM – UC – u tell me it won't hurt n I cant get pregnant n u know cuz u said u hv done this b4. I trust u Sam

08/27/2021 8:55 PM – PETERS – Yes babe you wil be super horny and wet when we do I promise

08/27/2021 8:55 PM – PETERS – I don't want to hurt you I love you

08/27/2021 8:56 PM – UC – I don't wanna get hurt. I get worried n stuff

08/27/2021 8:58 PM – PETERS – I know I won't hurt you

08/27/2021 8:58 PM – PETERS – I want you to be happy and feel pleasure not pain

08/27/2021 8:58 PM – PETERS – We will start slow and take as long as you want

08/27/2021 8:58 PM – PETERS – Lol

08/27/2021 8:58 PM – PETERS – I wish I could see your butt uncovered

08/27/2021 8:58 PM – UC – R u gonna wear something so I dont pregnant

08/27/2021 8:58 PM – PETERS – Yes I will

20. PETERS continues to engage the undercover on August 28, 2021 and August 29, 2021. On August 29, 2021, at approximately 11:05 AM, PETERS initiated communications with the undercover to confirm details for PETERS to meet the undercover later that afternoon.

21. On August 29, 2021 at approximately 3:25 PM, law enforcement officers from the FBI Pittsburgh Violent Crimes Against Children Task Force initiated a surveillance operation in the vicinity of the following target location: **REDACTED** with address **REDACTED** in Pittsburgh, Pennsylvania (hereinafter the “target location”). The target subject of the surveillance operation was RYAN PETERS and his vehicle (**TARGET VEHICLE**), a red Chevrolet Sonic Sedan bearing Pennsylvania license plate number LPR2231.³

22. The surveillance operation took place between approximately 3:25 PM and 5:00 PM on August 29, 2021. During the course of the operation, nine law enforcement officers, including your affiant and the undercover, observed the **TARGET VEHICLE** traveling on the streets nearby and adjacent to the target location. Specific observations of the **TARGET VEHICLE** and PETERS as the driver of the **TARGET VEHICLE** are discussed in detail below.

23. On August 29, 2021 at approximately 3:23 PM, a license plate reader (LPR) captured the **TARGET VEHICLE** turning from the McKees Rocks Bridge, travelling inbound on Route 65.

24. On August 29, 2021 at approximately 3:47 PM, your affiant observed the **TARGET VEHICLE** traveling northbound on **REDACTED** Street, crossing the intersection of **REDACTED** Street. Your affiant observed that the driver of the **TARGET VEHICLE** was wearing a hat similar to a “newsboy cap” and a mask over his face. On August 29, 2021 at approximately 3:50 PM, another law enforcement officer observed the **TARGET VEHICLE** driving in front of the

³ A search of a law enforcement database showed that a red Chevrolet Sonic Sedan bearing Pennsylvania license plate number LPR2231 (**TARGET VEHICLE**) was registered to RYAN PETERS and one other individual. Additionally, prior to the aforementioned search warrant executed at PETERS’ residence, law enforcement officers observed the **TARGET VEHICLE** parked at PETERS’ residence. Lastly, during the search warrant executed at PETERS’ residence, law enforcement officers observed the **TARGET VEHICLE** parked at the residence.

target location on South Tunnel Boulevard. This law enforcement officer observed that the driver of the **TARGET VEHICLE** was wearing a hat similar to a “newsboy cap.”

25. On August 29, 2021 at approximately 3:52 PM, your affiant, the undercover and another law enforcement vehicle observed the **TARGET VEHICLE** parked on REDACTED Street, facing southbound toward REDACTED Street. As the law enforcement officers drove by, your affiant and the undercover observed the driver of the **TARGET VEHICLE** wearing a “newsboy cap” and a mask which was pulled down under the driver’s mouth. The undercover also positively identified the driver as PETERS. The undercover recognized PETERS as the subject the undercover met in person during the previously-discussed search warrant executed at PETERS’ residence. The undercover also recognized PETERS as the individual pictured in the social media profile via which PETERS initiated contact with the undercover.

26. During the course of the surveillance operation which occurred between approximately 3:25 PM and 5:00 PM on August 29, 2021, PETERS engaged the undercover in the following conversation:

08/29/2021 3:49 PM – PETERS – You on your way

08/29/2021 3:50 PM – UC – R u here?

08/29/2021 3:51 PM – UC – U said 30 minutes haha

08/29/2021 3:51 PM – PETERS – Yeah I am

08/29/2021 3:51 PM – UC – Noooooooooo way

08/29/2021 3:51 PM – UC – Lolol

08/29/2021 3:51 PM – PETERS – Yeah

08/29/2021 3:53 PM – UC – Im comin down

08/29/2021 3:53 PM – PETERS – Send a pic of what you're looking at when u leave so I know where u r at

08/29/2021 3:56 PM – PETERS – Please

08/29/2021 3:57 PM – UC – REDACTED walkin now. Ill take a pic 4 u

08/29/2021 3:58 PM – UC – Ugh

08/29/2021 3:58 PM – PETERS – What?

08/29/2021 3:59 PM – UC – A [REDACTED] store near [REDACTED]? My apartment is like not door

08/29/2021 3:59 PM – UC – Nxt

08/29/2021 4:01 PM – UC – R u bein funny

08/29/2021 4:02PM – PETERS – No I'm not

08/29/2021 4:03 PM – UC – U r freakin me out.
I'll give u the pass code

08/29/2021 4:03 PM – UC – 75389#

08/29/2021 4:04:26 PM – PETERS – I didn't see you at all

08/29/2021 4:05 PM – PETERS – And I don't know the apartment building

08/29/2021 4:06 PM – UC – [REDACTED] tunnl next

08/29/2021 4:06 PM – UC – 2 [REDACTED]

08/29/2021 4:08 PM – PETERS – Can u meet me inside by the door

08/29/2021 4:08 PM – UC – Ya hurry

08/29/2021 4:08 PM – UC – Uup

08/29/2021 4:08 PM – PETERS – U excited or something

08/29/2021 4:09 PM – UC – Haha ya n scared

08/29/2021 4:12 PM – PETERS – Can you meet me on the corner there's no parking

08/29/2021 4:13 PM – PETERS – Please

08/29/2021 4:13 PM – UC – Use my dads spot in the lot n the side

08/29/2021 4:13 PM – UC – Wht r u drivin

08/29/2021 4:14 PM – UC – U r scarin me Sam. U rnt gonna hurt me r u

08/29/2021 4:14 PM – PETERS – Can u come down please

08/29/2021 4:14 PM – PETERS – No I'm not

08/29/2021 4:15 PM – UC – I came out. U lied. Said u were here

08/29/2021 4:15 PM – UC – Im in the lobby

08/29/2021 4:15 PM – PETERS – I was I'm just trying to find a spot

08/29/2021 4:16 PM – PETERS – Come outside

08/29/2021 4:17 PM – UC – No Im safe inside

08/29/2021 4:17 PM – PETERS – I have no where to park babe

08/29/2021 4:17 PM – UC – Imma bout to go 2 my room

08/29/2021 4:18 PM – UC – U rnt here

08/29/2021 4:19 PM – UC – My dad has a spot in the lot next to the front what r u talkn
bt

08/29/2021 4:20 PM – PETERS – Can I see a pic of you in the lobby please

08/29/2021 4:20 PM – UC – Noooo wy this is bad. U hv me freakd out

08/29/2021 4:21 PM – UC – stop

27. Next, on September 9, 2021, at approximately 7:51 PM, PETERS reinitiated contact with the undercover via another social media application. On this application, PETERS used the screenname “avaulion” and was listed as located in McKees Rocks, PA. PETERS stated to the undercover that he was sorry for scaring [her] and that he wanted to see [her].

28. On September 9, 2021, at approximately 7:52 PM, PETERS text messaged the undercover via the same telephone numbers they each previously used and engaged in the following conversation with the undercover:

09/09/2021 7:52 PM – PETERS – Hey [REDACTED] I'm sorry

09/09/2021 7:54 PM – PETERS – Please talk to me

09/09/2021 7:54 PM – PETERS – I really do love you

09/09/2021 7:56 PM – PETERS – Is this [REDACTED]

09/09/2021 7:59 PM – PETERS – Please say something I'm sorry

09/09/2021 8:05 PM – PETERS – You think I don't love you and you're mad at me right? What can I do to make it up to you

09/09/2021 8:07 PM – PETERS – I got scared you were messing with me so I went home

09/09/2021 8:16 PM – UC – U made me cry for a week

09/09/2021 8:16 PM – PETERS – I'm sorry my love what can I do

09/09/2021 8:16 PM – PETERS – Are you at your moms

09/09/2021 8:17 PM – UC – Ya. Not a good time rt now k.

09/09/2021 8:17 PM – UC – I can text u 4 a bit

09/09/2021 8:17 PM – PETERS – Wait please what's wrong

09/09/2021 8:17 PM – PETERS – And do u want to see me?

09/09/2021 8:17 PM – UC – Whats wrong????? U serious

09/09/2021 8:18 PM – PETERS – It's because of me

09/09/2021 8:18 PM – UC – My mum is around thats all

09/09/2021 8:18 PM – UC – Ya u left me. I ran around outside n u freaked me out like u were some crazy guy

09/09/2021 8:18 PM – PETERS – Well can you leave her house?

09/09/2021 8:19 PM – PETERS – I'm sorry babe I'm not I just got worried

09/09/2021 8:19 PM – PETERS – I'm really sorry I want to make it up to you

09/09/2021 8:19 PM – UC – K we can talk about it

09/09/2021 8:19 PM – UC – Sorry

09/09/2021 8:20 PM – PETERS – It's ok babe I am sorry I love you so much

09/09/2021 8:20 PM – UC – Wtf u had me sooo scared

09/09/2021 8:20 PM – PETERS – I am sorry I didn't see you I thought you were playing me

09/09/2021 8:21 PM – PETERS – If you want I can come get you

09/09/2021 8:21 PM – PETERS – For a bit

09/09/2021 8:22 PM – UC – No no no not tonight fr

09/09/2021 8:22 PM – PETERS – You sure babe

09/09/2021 8:22 PM – UC – U scared me 2 death

09/09/2021 8:22 PM – PETERS – I'm sorry baby

09/09/2021 8:23 PM – PETERS – I promise I won't hurt you, may I please see you

09/09/2021 8:23 PM – PETERS – I feel horrible

09/09/2021 8:23 PM – UC – Lemme think about it. K

09/09/2021 8:24 PM – PETERS – Ok babe cause I can get you for an hour or two if u want

09/09/2021 8:24 PM – PETERS – I wanna kiss you so bad

09/09/2021 8:25 PM – UC – Plse let me think bout it k. U made me soo sad

09/09/2021 8:25 PM – PETERS – Ok babe, so you might let me see u tonight?

09/09/2021 8:25 PM – UC – Nooooo. My mum is off n she watches me

09/09/2021 8:26 PM – PETERS – Oh where r u goona be 2 morrow

09/09/2021 8:27 PM – UC – I hv school n then I'm going camping all weekend. I wont be back til Sunday night 😞

09/09/2021 8:27 PM – PETERS – Ok babe, wish we could video chat

09/09/2021 8:28 PM – UC – U hv me sooo messed up rt now.

09/09/2021 8:28 PM – PETERS – I'm sorry babe

09/09/2021 8:29 PM – UC – I thot u were gonna hurt me or something cuz u wer actin crazy. Like wtf

09/09/2021 8:29 PM – UC – Sooo imma little sketched rt now

09/09/2021 8:29 PM – PETERS – I wasn't in sorry babe I just got scared

29. On September 13, 2021, at approximately 4:42 AM, PETERS text messaged the undercover to discuss meeting each other later that day. Later that day, at approximately 11:55 AM on September 13, 2021, PETERS arrived at the apartment complex in Allegheny County, Pennsylvania at the pre-determined time. At that time, agents arrested PETERS for violating 18 U.S.C. § 2242(b), attempted coercion and enticement of a minor to engage in sexual activity. Upon temporarily detaining PETERS, agents seized PETERS' cellular telephone (**TARGET DEVICE 2**) from him. The cellular telephone was unlocked. At this time, which was approximately 11:57 AM, the undercover sent a "test" text message to the telephone number via which the undercover had been communicating with PETERS. Agents witnessed PETERS' cellular telephone receive the "test" text message.

30. PETERS, who is 31 years old, admitted in a *Mirandized* and audio and video recorded interview that he was individual who has been communicating with the UC since August 2021, via social networking applications and through text messages. On September 13, 2021, PETERS drove his vehicle (**TARGET VEHICLE**) from his home to the apartment

complex, in Allegheny County, Pennsylvania to engage in sexual activity with the purported child.

31. The acts that PETERS planned to engage in with the purported child, as described in his chats with the undercover, are crimes punishable under Pennsylvania law, as described above at paragraph 3.

32. On September 13, 2021, United States Chief Magistrate Judge Patricia L. Dodge signed Criminal Complaint and Arrest Warrants at Magistrate No. 21-1857 accusing RYAN PETERS of violating Title 18, United States Code, Section 2422(b) which makes it a crime to use a facility or means of interstate commerce, such as the Internet and the telephone, to knowingly attempt to persuade, induce, entice, or coerce an individual who had not attained the age of 18 years to engage in sexual activity for which any person can be charged with a criminal offense. On September 13, 2021, RYAN PETERS was arrested, processed, and transported to the Allegheny County Jail where he remains in custody.

33. At the time which PETERS was detained in his vehicle (**TARGET VEHICLE**), agents observed and photographed condoms which PETERS told the undercover he would bring so that [she] would not get pregnant. Additionally, agents observed and seized two cellular telephones (**TARGET DEVICES 3 and 4**) in the vehicle. **TARGET DEVICES 2, 3 and 4** were seized, entered in to, and maintain in the custody of the FBI Pittsburgh Evidence Control Room located at 3311 E Carson Street, Pittsburgh, PA 15203. **TARGET VEHICLE** was towed and impounded at Critchlow Towing located at 1798 Babcock Blvd, Pittsburgh, PA 15209.

34. Based on my training and experience, individuals who possess, receive, distribute, and produce child pornography have a sexual attraction to children. They receive sexual

gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

35. Based on my training and experience, the majority of individuals who possess and produce child pornography collect sexually explicit materials, which may consist of photographs, videos, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

36. Based on my training and experience, individuals who possess and produce child pornography often seek out child pornography and child erotica using the Internet, often utilizing the Internet browsers on their cellular phone.

37. Based on my training and experience, individuals who possess and produce child pornography often seek out like-minded individuals, often through the Internet and e-mail, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P (Peer to Peer), e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles, and these vehicles can be accessed through the use of an internet capable device. This is often done using the internet, e-mail apps, and messaging apps on a user's cellular phone. For many of the same reasons, individuals who possess and produce child pornography often seek to communicate, through the internet, with children.

38. Based on my training and experience, individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the address books contained on a cellular phone or in an e-mail account, in the notes app of an iPhone, or in other various locations on a cellular phone.

DEFINITIONS

39. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

- a. “Minor,” as defined in 18 U.S.C. § 2256(1), means any person under the age of 18 years.
- b. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- c. “Child Pornography,” as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in “sexually explicit conduct,” as that term is defined in 18 U.S.C. § 2256(2).

d. “Visual depictions” include undeveloped film and videotape, data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. See 18 U.S.C. § 2256(5).

e. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

f. “Wireless telephone”: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the devices.

g. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as an electronic, magnetic, optical, electrochemical, or other high speed data processing devices

performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such devices.

h. “Digital camera”: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

i. “Internet Service Providers” or “ISPs,” are businesses that enable individuals to obtain access to the Internet. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines, provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers, remotely store electronic files on their customers’ behalf, and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, electronic mail transaction information, posting information, account application information, and other information both in computer data and written format.

j. An “Internet Protocol” or “IP” address is a unique numeric address used by computers or cellular telephones on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer

connected to the Internet must have an assigned IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a particular range of IP addresses. When a customer connects to the Internet using an ISP service, the ISP assigns the computer an IP address. Any and all computers using the same ISP account during that session will share an IP address. The customer's computer retains the IP address for the duration of the Internet session until the user disconnects. The IP address cannot be assigned to a user with a different ISP account during that session. When an Internet user visits any website, that website receives a request for information from that customer's assigned IP address and sends the data to that IP address, thus giving the Internet user access to the website.

k. "Internet": The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

40. Based on my knowledge, training, and experience, I know that electronic devices, such as the **TARGET DEVICES**, can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

41. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the **TARGET DEVICES** were used, the purpose of their use, who used them,

and when. There is probable cause to believe that this forensic electronic evidence of the target offenses will be on the **TARGET DEVICES** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file.
- b. As explained herein, information stored within a smartphone may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a smartphone (e.g., communications, images and videos, transactional information, records of session times and durations, and internet history) can indicate who has used or controlled the smartphone. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. Further, smartphone media activity can indicate how and when the smartphone was accessed or used. Additionally, some information stored within a smartphone may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a smartphone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The geographic and timeline information described herein may either inculcate or exculpate the user of the Device. Last, information stored within a smartphone may provide relevant insight into the smartphone user’s state of mind as it relates to the offense under investigation. For example, information within the smartphone may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., deleting images of contraband that nevertheless remain in caches

unknown to the user or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a smartphone works may, after examining this forensic evidence in its proper context, draw conclusions about how smartphones were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a smartphone is evidence may depend on other information stored on the smartphone and the application of knowledge about how a smartphone behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a smartphone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

42. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

REQUEST TO USE BIOMETRIC CHARACTERISTICS TO ACCESS DEVICES

43. The warrant I am applying for would permit law enforcement to obtain from PETERS the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock the **TARGET DEVICES** subject to search pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the

device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, the **TARGET DEVICES** were in Ryan Peters' possession and are reasonably believed to belong to Peters. The passcode or password that would unlock the **TARGET DEVICES** subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the **TARET DEVICES**, making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered in

the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. Due to the foregoing, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of PETERS, who is reasonably believed by law enforcement to be a user of the devices, to the fingerprint scanner of the **TARGET DEVICES**; (2) hold the **TARGET DEVICES** in front of the face of PETERS and activate the facial recognition feature, for the purpose of attempting to unlock the **TARGET DEVICES**, in order to search their contents as authorized by this warrant.

CONCLUSION

44. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **TARGET ITEMS** described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Samantha Shelnick

Samantha Shelnick
Special Agent
Federal Bureau of Investigation

Sworn to before me telephonically
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 17th day of September 2021.



HONORABLE PATRICIA L. DODGE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED (TARGET ITEMS)

- (1) Samsung Cellular Telephone, IMEI 350121675480685,
- (2) Motorola Moto G Power Cellular Telephone, XT2117-1, Serial Number ZY22CTDQM6, IMEI 356889113879890,
- (3) LG K51 Cellular Telephone, LM-K500UM, Serial Number 009WIRW2724902, IMEI 354591111029583,
- (4) Samsung Galaxy A11 Cellular Telephone, SM-A115U, Serial Number R95N80MQ1ZM, IMEI 356425115244151, and
- (5) 2015 Chevrolet Sonic Sedan, License Plate LPR2231, Vehicle Identification Number (VIN) 1G1JC5SH9F4180911 (“the **TARGET ITEMS**”).

This warrant authorizes the examination of the above-listed property—electronic devices and a vehicle—and the extraction from that property of electronically stored information and items specifically described in Attachment B.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

The particular things to be seized and searched include all records, in whatever format, stored on the **TARGET DEVICES** or in the **TARGET VEHICLE**, fully described in Attachment A that relate to 18 U.S.C. § 2252(a), relating to the possession of child pornography, and 18 U.S.C. § 2422(b), enticement, and involve PETERS, to include:

1. Any depictions of child pornography as defined in 18 U.S.C. § 2256(8), any visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), and any child erotica.

2. Any and all software and apps, including programs to run operating systems, applications, utilities, compilers, interpreters, and communications programs, including: mapping apps, photography apps, travel apps, email apps, and any applications that have messaging capabilities.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including e-mail messages, text messages, instant messages, chat logs, and other digital data files) pertaining to location information.

4. In any format and medium, all photographs, images, and videos contained on the **TARGET DEVICES**.

5. Any and all electronic address books, names, and lists of names and addresses of individuals on the **TARGET DEVICES** who PETERS may have communicated with.

6. Any and all documents, records, or correspondence, pertaining to the ownership and use of the **TARGET DEVICES** described above, such as saved

usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, text messages, photographs, and correspondence, including the text messages with the undercover described in this affidavit or with anyone else in violation of 18 U.S.C. § 2422(b).

7. Passwords, encryption keys, and other access devices that may be necessary to access information stored on the **TARGET DEVICES** or elsewhere. Any and all passwords and other data security devices designed to restrict access to, hide, or destroy software, documentation, or data. Data security devices may consist of software or other programming code. Any and all data which would reveal the presence of malware, viruses or malicious codes located on the computer storage media.

8. Records of, or information about, the **TARGET DEVICES’** internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

9. Records evidencing the use of the Internet Protocol Addresses, including records of Internet Protocol Addresses used by the device and Internet Protocol Addresses used by computers that the **TARGET DEVICES** connected to.

10. Items evidencing a violation of 18 U.S.C. § 2422(b) located in the **TARGET VEHICLE** which were specifically discussed during conversations between PETERS and the undercover, to include, but not limited to, condoms.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search for the **TARGET DEVICES**, described in Attachment A, law enforcement personnel are authorized if necessary, to (1) press or swipe Ryan Peters' fingers (including thumbs) to the fingerprint scanner of the **TARGET DEVICES**; and (2) present Ryan Peters' face to the camera of the **TARGET DEVICES** found in the possession of Peters for the purpose of attempting to activate the facial recognition feature and unlock the **TARGET DEVICES** via biometric security in order to search the contents as authorized by this warrant.

IN THE COURT OF COMMON PLEAS, ALLEGHENY COUNTY PENNSYLVANIA

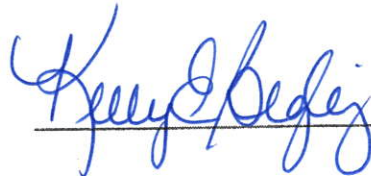
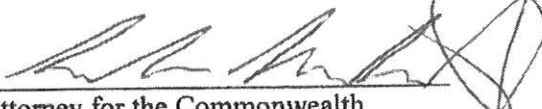
CRIMINAL DIVISION

ORDER OF COURT

AND NOW, to wit, this **28th day of September, 2021**, the Court finds that good cause is contained within the affidavit to order the nondisclosure of this warrant and affidavit of probable cause to the account holder of the account that is the subject of this warrant for a period of one year from the date of this order (subject to further extension granted by this court). AND NOW, to wit **Microsoft Corporation USA.** is hereby ORDERED and DIRECTED to remain confidential the attached warrant and affidavit of probable cause from the account holder of the account subject to the search warrant for a period of one year from the date of this order (subject to further extension granted by this court).

(OneDrive Account: Jalestall@gmail.com)



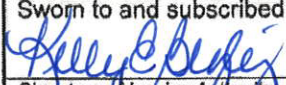
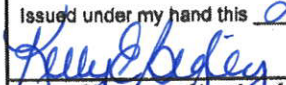
BY THE COURT,


_____

Attorney for the Commonwealth

EXHIBIT

3

Commonwealth of Pennsylvania				APPLICATION FOR SEARCH WARRANT AND AUTHORIZATION	
COUNTY OF ALLEGHENY					
Docket Number (Issuing Authority):	Police Incident Number: CTF#21-027	Warrant Control Number:			
Detective Scott Klobchar	Allegheny County Police Dept	412-298-9311	09/28/2021		
AFFIANT NAME	AGENCY	PHONE NUMBER	DATE OF APPLICATION		
IDENTIFY ITEMS TO BE SEARCHED FOR AND SEIZED (Be as specific as possible):					
Items to be Seized associated with the Microsoft OneDrive Account associated with email address: <u>Jalestall@gmail.com</u> – between the dates of 08/17/2020 through present. (Ryan Mark PETERS, D/O/B/ REDACTED 1989)					
****SEE CONTINUATION PAGE****					
SPECIFIC DESCRIPTION OF PREMISES AND/OR PERSON TO BE SEARCHED (Street and No., Apt. No., Vehicle, Safe Deposit Box, etc.):					
Microsoft Corporation USA (Custodian of Records) 1 Microsoft Way Redmond, WA 98052-6399					
NAME OF OWNER, OCCUPANT OR POSSESSOR OF SAID PREMISES TO BE SEARCHED (If proper name is unknown, give alias and/or description):					
Microsoft Corporation USA					
VIOLATION OF (Describe conduct or specify statute): Title 18 Sec 6312- Sexual Abuse of Children				DATE(S) OF VIOLATION: 08/17/2020 - Present	
<input checked="" type="checkbox"/> Warrant Application Approved by District Attorney – DA File No. <u>322419</u> <small>(If DA approval required per Pa.R.Crim.P. 2002A with assigned File No. per Pa.R.Crim.P. 107)</small> <input checked="" type="checkbox"/> Additional Pages Attached (Other than Affidavit of Probable Cause) <input checked="" type="checkbox"/> Probable Cause Affidavit(s) MUST be attached (unless sealed below) Total number of pages: <u>10</u>					
TOTAL NUMBER OF PAGES IS SUM OF ALL APPLICATION, PROBABLE CAUSE AND CONTINUATION PAGES EVEN IF ANY OF THE PAGES ARE SEALED					
The below named Affiant, being duly sworn (or affirmed) before the Issuing Authority according to law, deposes and says that there is probable cause to believe that certain property is evidence of or the fruit of a crime or is contraband or is unlawfully possessed or is otherwise subject to seizure, and is located at the particular premises or in the possession of the particular person as described above.					
 Signature of Affiant		Allegheny County Police Dept		452	
		Agency or Address if private Affiant		Badge Number	
Sworn to and subscribed before me this <u>28th</u> day of <u>September 2021</u> Mag. Dist. No. <u>5th District</u>					
 Signature of Issuing Authority		<u>436 Grant Street Pgh PA 15219</u> Office Address			
SEARCH WARRANT TO LAW ENFORCEMENT OFFICER:		WHEREAS, facts have been sworn to or affirmed before me by written affidavit(s) attached hereto from which I have found probable cause, I do authorize you to search the premises or person described, and to seize, secure, inventory and make return according to the Pennsylvania Rules of Criminal Procedure.			
<input checked="" type="checkbox"/> This Warrant shall be served as soon as practicable and shall be served only between the hours of 8AM to 10PM but in no event later than: * <input type="checkbox"/> This Warrant shall be served as soon as practicable and may be served any time during the day or night but in no event later than: ** <u>10:37am</u> M, o'clock <u>September 30, 2021</u>					
* The issuing authority should specify a date not later than two (2) days after issuance. Pa.R.Crim.P. 2005(d). ** If the issuing authority finds reasonable cause for issuing a nighttime warrant on the basis of additional reasonable cause set forth in the accompanying affidavit(s) and wishes to issue a nighttime warrant, then this block shall be checked. Pa.R.Crim.P. 2006(g).					
Issued under my hand this <u>28th</u> day of <u>September, 2021</u> at <u>10:37am</u> M, o'clock.					
 Signature of Issuing Authority		<u>5th Judicial District</u> Mag. Dist. or Judicial Dist. No.		<u>Jan 2028</u> Date Commission Expires:	
Title of Issuing Authority: <input type="checkbox"/> District Justice <input checked="" type="checkbox"/> Common Pleas Judge <input type="checkbox"/>					
<input type="checkbox"/> For good cause stated in the affidavits(s) the Search Warrant Affidavit(s) are sealed for _____ days by my certification and signature. (Pa.R.Crim.P. 2011)					
(Date) (SEAL)					
Signature of Issuing Authority (Judge of the Court of Common Pleas or Appellate Court Justice or Judge).					

TO BE COMPLETED BY THE ISSUING AUTHORITY

Commonwealth of Pennsylvania



APPLICATION FOR SEARCH WARRANT CONTINUATION PAGES

COUNTY OF Allegheny

Docket Number
(Issuing Authority):Police Incident
Number: CTF#21-027Warrant Control
Number:**Continuation of:**☒ Items to be searched
and seized☐ Description of premises/person(s)
to be searched☐ Owner/ Occupant☐ Violations**Items to be seized:****(To be produced by Microsoft Corporation US.):**

- (a) All account information, including: full name provided by the user, telephone numbers provided by user, physical address (including city, state, and zip-code), email address provided by the user, time and date of account registration (including length of service), type of account (Free/Paid/Business, and if paid, payment information), records of session times and durations, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, last seen IP address of computers linked to the account; methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- (b) All records or other information stored by an individual using the account, including videos, images, documents, files, email addresses, and contact lists;
- (c) All records pertaining to communications between Microsoft OneDrive and any person regarding the account, including contacts with support services and records of actions taken;
- (d) All user data to include content and non-content data including deleted content, to included images, videos, communications and messages sent or received. Any content data stored within the personal vault of the requested OneDrive Account.

All information that constitutes fruits, evidence and instrumentalities of violations of PA Title 18 §6312 – Sexual Abuse of Children, including the following: Images and videos that depict the possession, receipt, or distribution of child pornography, as defined in PA Title 18 §6312, or attempts to do so.

- (e) Any evidence that would tend to show the true identities of the persons committing these offenses, or their locations, including but not limited to IP addresses, and subscriber and account information. All activity logs and IP logs, including all records of the IP addresses that logged into the accounts or uploaded files into the accounts.
- (f) All account information, including: full name; email address; telephone number; length of service; status of account (whether the account is active or disabled); settings on account to include if the account or its folders are open to the public to view and/or upload files to; type of account; payment information; IP addresses for account login and uploads; last seen IP addresses of computers linked to the account; mobile device information;
- (g) All logs of devices and accompanying serial or model numbers and other identifying numbers to include dates of activation, registration, deactivation, or use;
- (h) Images and videos that depict the possession, receipt, or distribution of child pornography, more specifically the “file path” of any child pornographic images as defined in PA Title 18 §6312, contained within the OneDrive account associated with Jalestall@gmail.com

[Signature] 9/28/21

Page 2 of 10 Pages

KJB
9-28-2021

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number

Police Incident

Warrant Control

(Issuing Authority):

Number: CTF#21-027

Number:

PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:Social security numbers and financial information (e.g. PINs) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.

Your affiant is Detective Klobchar with the Allegheny County Police Department currently assigned to the FBI's Child Exploitation and Human Trafficking Task Force which is comprised of Federal and Local Law Enforcement. Your affiant is also a member of the Delaware County Internet Crimes Against Children (ICAC) Taskforce. Previously your affiant was assigned as a Detective to the Allegheny County Police Department Child Abuse / Sex Assault unit. Your affiant has been in Law Enforcement for over 19 years. I have spent over 11 of those years being assigned to various investigative units within the Allegheny County Police Department to include, narcotics, homicide and child abuse units.

Your affiant is familiar with investigations involving the exploitation of children both via the internet and in person. Your affiant is also familiar with investigations involving child pornography images. As part of my duties, your affiant investigates violations involving online exploitation of children, violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors. Your affiant has participated in the execution of numerous search warrants and arrests relating to sexual abuse of children.

Definition of "Child Pornography" (as defined in section 6312 of the PA Crimes Code) - any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of 18 years engaged in a prohibited sexual act or in the simulation of such act.

Definition of prohibited sexual act (as defined in section 6312 of the PA Crimes Code) - sexual intercourse, masturbation, sadism, masochism, bestiality, fellatio, cunnilingus, lewd exhibition of the genitals or nudity if such nudity is depicted for the purpose of sexual stimulation or gratification of any person who might view that depiction.

IP Address : An IP address is analogous to a phone number in that both serve as a unique identifier for a particular device. Similar to how a phone number is assigned to a telephone device, an IP address is assigned to a specific computer. Furthermore, each router that a device uses to connect to the Internet also has an IP address assigned by the Internet Service Provider ("ISP"), comparable to how a phone number is assigned by the phone provider. Similar to how a person would dial a given number to reach a specific individual, the assigned IP address allows various devices connected to the Internet to "talk" to each other so that data can be shared among them. Most machines will also have a Domain Name that are easier for people to remember.

Domain Name: This is the unique name that identifies an Internet Site. Domain names always have two or more parts separated by periods. The left side of the domain name is referred to as the *Second Level Domain* (SLD), while the right side of the Domain Name is referred to as the *Top Level Domain* (TLD). When you access a website, the domain name is translated to an IP address, which defines the server where the website located. This translation is performed dynamically by a service called DNS, which stands for "*Domain Name System*."

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

Affiant Signature

Date

9-28-21

Issuing Authority Signature

Date

(SEAL)

Page 3 of 10 Pages

KOB
9-28-2021

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number

Police Incident

Warrant Control

(Issuing Authority):

Number: CTF#21-027

Number:

PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:

Social security numbers and financial information (e.g. PINs) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.

Domain names serve as easily memorized names for websites and other services on the Internet. However, computers access Internet devices by their IP addresses. DNS translates domain names into IP addresses, allowing you to access an Internet location by its domain name.

American Registry of Internet Numbers (ARIN)- is a non-profit organization, responsible for managing the Internet numbering resources for Canada, the United States, and many Caribbean and North Atlantic islands. Other registry organizations are separately responsible for registering and maintaining domain names, which are commonly used unique identifiers that are translated into numeric addresses (IP Addresses). IP Addresses are globally unique numeric identifiers that computers use to identify hosts and networks connected to the Internet. Open structures and processes are maintained in all of the ARIN's daily operations to ensure that the needs of the Internet Community are adequately met.

GOOGLE ACCOUNT: A Google Account is a username and password that can be used to log in to consumer Google applications like Docs, Sites, Maps, and Photos. Many Google accounts end in @gmail.com however it isn't necessary to have a Gmail account in order to have a Google account. Google Photos is a photo sharing and storage service which Google account users can access to share and store photographs and videos.

Microsoft OneDrive: is the cloud storage service that Microsoft offers to store all your files securely in one place, which you can then access from virtually anywhere. The service works like a traditional external drive, however you can access it through the internet. The service works across various devices and platforms, allowing a user to can create a file on one device and access it on another (desktop computer, laptop, tablet, or phone). Also, OneDrive makes it easy to share content with other people and collaborate in real-time using the Microsoft 365 integration. OneDrive Basic allows subscribers to use this service free of charge up to 5GB of data.

SNAPCHAT: Snapchat is a multimedia messaging app. One of the key features of Snapchat is that it allows users to share photographs and short video clips between users. One principle feature of Snapchat is that when a photo or video clip is sent, it can only be viewed for a short period of time, before they become inaccessible to the intended recipient. This can be circumvented by photographing the image through external means.

National Center For Missing and Exploited Children (NCMEC)- NCMEC operates the Cyber Tipline which was established by Congress to process reports of child sexual exploitation (including child pornography, online enticement, and contact offenses). The NCMEC reviews these reports and shares them with the appropriate law enforcement agency or *Internet Crimes Against Children (ICAC)* task force. In addition to the information provided by the reporting party, NCMEC typically adds geolocation information (if appropriate) and cross-references identifying information such as email address, username, or IP address with existing Cyber Tipline Reports.

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.


Affiant Signature

9/28/21
Date

Issuing Authority Signature

Date

(SEAL)

Page 4 of 10 Pages

KD
9-28-2021

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number

Police Incident

Warrant Control

(Issuing Authority):

Number: CTF#21-027

Number:

PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:Social security numbers and financial information (e.g. PINs) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa. Code §§ 213.1 - 213.7.

On 08/17/2020, the National Center for Missing and Exploited Children (NCMEC) received a Cybertip, (CYBERTIP # 76695176) from Snapchat. Snapchat reported that a user, utilizing the screenname: **jalestal** had uploaded an image of suspected child pornography on 08/17/2020 at 05:42:02 UTC. Snapchat provided an IP Address that was captured by Snapchat on 08/14/2020 at 02:50:24 UTC, and identified that IP Address: **REDACTED**.155. Snapchat also reported that this account was associated with cellular telephone number (412) 512-6248.

Your affiant viewed the uploaded image and confirmed that it depicted a prepubescent female child exposing her genitals in a sexual act and/or pose.

On 09/16/2020, the National Center for Missing and Exploited Children (NCMEC) received a Cybertip, (CYBERTIP # 79623247) from Dropbox. Dropbox reported to NCMEC that a person using the Screen/User Name: **Jalestal Divine**, uploaded eleven (11) images of suspected child pornography to their Dropbox account. Dropbox provided that this user registered this Dropbox account using IP address: **REDACTED**.155 on 08-03-2020 at 22:08:18 UTC. Dropbox identified the Email account associated with this account as: **jalestall@gmail.com**.

Dropbox reported that they had viewed the entire contents of the uploaded files. Your affiant also previewed the reported uploaded files and confirmed that they depicted prepubescent aged female children engaged in sexual acts and/or exposing their genitals in a sexual act and/or pose.

Based on the fact that the National Center for Missing and Exploited Children (NCMEC), had reported receiving two separate Cybertips from different electronic service providers, which reported the same IP Address of: **REDACTED**.155, it was believed by your affiant that both accounts were operated by a single user. A check of the IP Address: **REDACTED**.155 through *IP2Location.com*, yielded results for belonging to Verizon communications.

On 04/29/2021, a search warrant was applied for and obtained for the subscriber information on the IP Address: **REDACTED**.155. The search warrant was signed by the Honorable Judge David Cashman. The search warrant was executed on Verizon communications and as a result, Verizon provided the following information.

Verizon provided the subscriber information as: **REDACTED** with a service address of **REDACTED** St McKees Rocks, PA 15136 and provided an email that was linked to the Verizon account, which Verizon identified as, **jalestall@gmail.com**. According to Verizon records, the address of **REDACTED** St McKees Rocks, PA 15136, would have been the service address of IP Address: **REDACTED**.155 at the time both Cybertips were reported.

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

Affiant Signature

9/28/21

Issuing Authority Signature

Date

(SEAL)

Page 5 of 10 Pages

KB
9-28-2021

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number

Police Incident

Warrant Control

(Issuing Authority):

Number: CTF#21-027

Number:

PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:*Social security numbers and financial information (e.g. PINs) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.*

Investigators began gathering intelligence on current potential residents, residing at [REDACTED] St McKees Rocks, PA 15136. As a result, it was learned that, **Ryan Mark PETERS**, was listed as currently residing at this address. A check of **PETERS** through JNET, yielded [REDACTED] St McKees Rocks, PA 15136 as the address, he lists on his Pennsylvania Driver's License. On 07/26/2021 US Postal Inspectors confirmed that **Ryan PETERS** and [REDACTED] are currently receiving US Mail at this address.

A criminal history check of **PETERS**, reflected that he has prior arrests in New York and Pennsylvania, to include a 2013 Pennsylvania arrest for the following offenses: **Statutory Sexual Assault, Aggravated Indecent Assault, Unlawful contact with a minor, Corruption of Minors, and IDSI**. A criminal complaint was obtained regarding the aforementioned charges. Upon reviewing the criminal complaint, it was learned that on 03/07/2013, the Pennsylvania State Police filed the above charges, subsequent to an investigation, in which **PETERS** was alleged to have engaged in sexual intercourse with a 13 year-old female, when he was 22 years-old.

A check of the telephone number, (412) 512-6248, through a law enforcement database, yielded results for belonging to **Ryan M PETERS**, [REDACTED] 1989, of [REDACTED] St McKees Rocks, PA 15136.

Based on the fact that both Cybertips were associated with screen name, "**Jalestal**", I conducted a check of the screenname **JALESTAL** through Facebook, to determine if that username was associated with a Facebook account. As a result, I located a Facebook page under the name, "**Ryan Jalestal Peters**". This Facebook account displayed a Facebook profile picture that was extremely similar to the driver's license photograph of **Ryan M. PETERS**, [REDACTED] 1989). In the "about" section of the Facebook profile, it stated that he attended **Clymer Central School**. While reviewing the previously mentioned criminal complaint, filed on 03/07/2013, the complaint states that **PETERS** had stated that he graduated from high school in **Clymer, NY**.

Based on the aforementioned information, I applied for and obtained a search warrant for the residence of [REDACTED] St McKees Rocks, PA 15136. The search warrant was obtained to search for and seize electronic devices for child pornography.

On Friday August 06, 2021 members of the FBI Pittsburgh Child Exploitation and Human Trafficking Task Force executed a search warrant at the residence of [REDACTED] St Pittsburgh, PA 15136. **Ryan PETERS** was present at the time of the execution. As a result of the search warrant several electronic devices were seized. One of these items was identified as a **Samsung cellular telephone**, (IMEI#350121675480685), was recovered from inside a kitty litter box.

This **Samsung** cellular telephone was forensically examined by FBI personnel at the FBI Pittsburgh Field Office. During the analysis, a **Microsoft OneDrive** was installed on the cell phone which contained content depicting child pornography.

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

 9/28/21
 Date

Issuing Authority Signature

Date

(SEAL)

Page 6 of 10 Pages

 KB
 9-28-2021

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number

Police Incident

Warrant Control

(Issuing Authority):

Number: CTF#21-027

Number:

PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:

Social security numbers and financial information (e.g. PINs) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.

One of the videos located within Microsoft OneDrive, depicted a pre-pubescent aged female posing naked in sexual acts and/or poses. A separate video located in the Microsoft OneDrive account depicted a prepubescent aged female engaged in vaginal intercourse, with what appeared to be an adult male.

The Microsoft OneDrive account was associated with the email address: Jalestall@gmail.com.

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND ONEDRIVE

The term "computer" as used herein is defined in 18 Pa.C.S. § 7601, an electronic, magnetic, optical, hydraulic, organic or other high-speed data processing device or system which performs logic, arithmetic or memory functions and includes all input, output, processing, storage, software or communication facilities which are connected or related to the device in a system or network.

The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web ("www") is a functionality of the Internet which allows users of the Internet to share information.

With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.

Your affiant knows based on research, personal knowledge and experience that OneDrive is a file hosting service operated by Microsoft Corporation, headquartered in Redmond, Washington. OneDrive is a file syncing, hosting service that offers cloud storage, file synchronization, personal cloud, and client software access. It allows users to share files on computers, phones, tablets, and the OneDrive website, and permits its users to store files on OneDrive's servers. OneDrive stores, processes and transmits the account holder's files (including photos, videos, structured data, and emails), which allows users to access a file from virtually anywhere).

In September 2019 Microsoft announced Personal Vault. It is a protected area in OneDrive where users can store their most important or sensitive files and photos without sacrificing the convenience of anywhere access. Personal Vault has a strong authentication method or a second step of identity verification, such as fingerprint, face, PIN, or a code sent via email or SMS.

OneDrive also supports version history, so files deleted from the OneDrive folder may be recovered from any of the synced computers. OneDrive supports multi-user version control, enabling several users to edit and re-post files without overwriting versions.

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

[Signature]
Affiant Signature

9/28/21
Date

Issuing Authority Signature

Date

(SEAL)

Page 7 of 10 Pages

KB
9-28-2021

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number

Police Incident

Warrant Control

(Issuing Authority):

Number: CTF#21-027

Number:

PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:

Social security numbers and financial information (e.g. PINs) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.

OneDrive also offers users a free account with a set storage size, and paid subscriptions for accounts with more capacity. OneDrive offers computers apps for android, Windows Phone, and iOS mobile devices, Windows and macOS computers as well as Xbox gaming systems.

In general, providers like OneDrive ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account.

In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTOR

Your Affiant knows from training and experience that the following characteristics are prevalent among individuals who collect child pornography:

The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

The majority of individuals who collect child pornography collect explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless fuel their sexual fantasies involving children.

The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to, peer to peer, e mail, bulletin boards, Internet relay chat, newsgroups, instant messaging, and other similar vehicles.

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO L.W. DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

Affiant Signature

 9/28/21
Date

Issuing Authority Signature

Date

(SEAL)

Page 8 of 10 Pages

 KB
9-28-2021

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number
(Issuing Authority):Police Incident
Number: CTF#21-027Warrant Control
Number:**PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:**

Social security numbers and financial information (e.g. PINs) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.

The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

The majority of individuals who collect child pornography often correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. These contacts are maintained as a means of personal referral, or exchange. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or on scraps of paper.

The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage.

Your affiant believes that evidence will be contained with **Microsoft OneDrive**, which will lead to the identity of the individual/s who possess child pornography. Your affiant believes that there is probable cause to believe that these items constitute evidence and instrumentalities of violation for the crime of **PA Title 18, Section 6312, Sexual Abuse of Children**. Your affiant learned through training and experience, those persons engaged in the distribution and possession of pornographic/child pornographic materials often maintain collections of such material and that such material is used as a resource for furtherance of the exploitation of juveniles. The collections are kept by these persons for long periods of times, years at times.

IN SUPPORT OF NON-DISCLOSURE COURT ORDER: Due to the sensitive nature of this case, the notification to the account holder(s) regarding the existence of this search warrant at this time would undermine the ongoing criminal investigation, jeopardize the prosecution's right to prosecute its case relating to the criminal investigation, and jeopardize the right of the suspect(s) to be charged in this a matter from receiving a fair trial.

Furthermore, the affiant shows unto the court that no suspects identified in this criminal investigation have been charged. So the notification to the users of the account(s) regarding the existence of this search warrant could jeopardize the State's ability to bring the responsible parties to justice, or allow an opportunity for the suspect(s) to flee, tamper with evidence, or change patterns of behavior.

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

[Signature] *9/28/21* *[Signature]* *[Date]* (SEAL)
Affiant Signature Date Issuing Authority Signature Date
Page 9 of 10 Pages

KB
9-28-2021

Commonwealth of Pennsylvania

AFFIDAVIT OF
PROBABLE CAUSE

COUNTY OF ALLEGHENY

Docket Number
(Issuing Authority):Police Incident
Number: CTF#21-027Warrant Control
Number:**PROBABLE CAUSE BELIEF IS BASED UPON THE FOLLOWING FACTS AND CIRCUMSTANCES:**

Social security numbers and financial information (e.g. PINs) should not be listed. If the identity of an account number must be established, list only the last four digits. 204 Pa.Code §§ 213.1 - 213.7.

Based on the above, the affiant requests approval of a separate court order prohibiting Microsoft Corporation from disclosing the existence of this search warrant to the account holder(s) who are the subject of this warrant

Your affiant asserts the named items are evidence of criminal activity and as such are subject to search and seizure.

I, THE AFFIANT, BEING DULY SWORN ACCORDING TO LAW, DEPOSE AND SAY THAT THE FACTS SET FORTH IN THE AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION AND BELIEF.

[Signature]
Affiant Signature

9/28/21
Date

[Signature]
Issuing Authority Signature

9-28-2021
Date (SEAL)

Page 10 of 10 Pages